August 30th 2016

MASTER THESIS

IPV4 VS IPV6 ANYCAST CATCHMENT: A ROOT DNS STUDY

Muhammad Arif Wicaksana

Telematics
Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS)
Design and Analysis of Communication System (DACS)

Examination committee
Prof. dr. ir. Aiko Pras
Dr. Ricardo de Oliveira Schmidt
Wouter B. de Vries, M.Sc.

UNIVERSITY OF TWENTE.

Abstract

Anycast has been extensively used by DNS Root Server operators to improve performance, resilience, and reliability. In line with the migration towards IPv6 networks, 9 out of 11 anycasted Root Servers are running on both IPv4 and IPv6 (dual-stack mode) today. Ideally, both protocols should provide similar performances. Problem arises since operators may have different peering policies for IPv4 and IPv6 networks, which leads to different catchment areas for the same service and potentially different quality of service. In this thesis, we analyze the IPv4 and IPv6 catchments of anycasted Root Servers from control-plane perspective between February 2008 to June 2016 using BGP data from RIPE RIS. We study the evolution and the differences of the catchment areas over the time. We also develop visualization tool to help operator assess their catchment areas. While we specifically study DNS Root Server, our methodology can be applied to other anycast services as well.

Acknowledgements

First and foremost, I would like to express my gratitude to Ricardo de Oliveira Schmidt for giving me the opportunity to work on this subject and providing support, feedback, and suggestions to improve my thesis. I sincerely thank to the other examination committee, Aiko Pras and Wouter de Vries. Additionally, I also would like to thank Jair, Luuk, and Wouter for being really helpful when I was working at the office. In particular for Jair, who greatly helped me preparing my presentation.

I gratefully acknowledge the MCIT of Indonesia for funding my study, which allows me to make one of my dreams comes true. I am also grateful to all kind people who helped me throughout my master study at University of Twente whom I cannot mention one by one. May God reward you and accept your good deeds.

Last but not least, I would like to thank my family for supporting me, and especially Pamahayu Prawesti for her patience and unconditional love.

Contents

List of Abbreviations

AS: Autonomous System

ASN: Autonomous System Number

BGP: Border Gateway Protocol

BMP: BGP Message Protocol

CDN: Content Distribution Network

DDoS: Distributed Denial of Service

DNS: Domain Name Service

FQDN: Fully Qualified Domain Name

IP: Internet Protocol

IPv6: Internet Protocol version 6

MRT: Multi-threaded Routing Kit

RFC: Request for Comment

RIPE: Réseaux IP Européens

RIS: Routing Information Service

TLD: Top-level Domain

List of Figures

List of Tables

1. Introduction

IP anycast [50] is a technique to share the same IP address among multiple nodes in multiple locations relying on the routing system to map clients to an anycast node (*one-to-any* connection) based on certain parameters, *e.g.*, server proximity, server load, and so on. It started to gain momentum after the DDoS attack targeting all DNS Root Servers on 2002, causing 9 out of 13 Root Servers to be out of service for a moment. The attack caused the link to be congested, leading to unreachable service experienced by user, even though the servers itself remained fully operational. The use of IP anycast enabled Root Servers operators to mitigate such problem. By spreading their instances around the globe, the DDoS attack can be localized to a certain instance, while instances on the other locations remains functional. Another benefit of anycast is to bring the service closer to the users thus reducing service response time, while at the same time keeping the configuration at user side simple. Today, IP anycast is also employed by other distributed services as well, such as CDN, web hosting, and so on.

Despite of its simplicity, IP anycast is difficult to manage. It is because IP anycast completely depends on the routing system–typically BGP–to select the serving anycast node. BGP itself is well-known for its complexity; mainly because it does not route packets solely based on the shortest path, but also takes into account some other considerations in the form of routing policies. Improper BGP configuration could lead to suboptimal routing, causing worse quality of service. For critical service such as DNS, this is a very important issue, since routing configuration also contributes to the latency experienced by users. DNS is a fundamental Internet protocol where many other protocols are relying on it to operate properly (*e.g.*, mail, web). Slow DNS query results in slow response time to them as well. On another side, the deployment strategy of IPv6 to smoothly replace IPv4 allows the IPv4 and IPv6 coexistence in a network. Ideally both protocols should have similar performances. However, this is not always the case. Study from [6] that performed measurements against 100 popular dual-stacked websites shows that the performances are sometimes different. Furthermore, performance over IPv6 paths is comparable to those over IPv4 if the AS-level paths are the same. However, it can be much worse if the AS-level paths differ [27]. It shows that having the knowledge over the global Internet for both IPv4 and IPv6 is important to ensure the anycast service is running similarly.

This thesis assesses the differences between IPv4 and IPv6 service coverage (*catchment areas*) from anycast service. DNS Root Servers is used as the case study, primarily because DNS is the pioneering application that heavily uses anycast. Nevertheless, the methodology used in this thesis can be easily applied to other IP-anycast services as well. Here, this thesis is focused on the control plane aspect, *i.e.*, BGP as the routing system used to deliver packets globally. We obtained data from RIPE RIS project

[53] that collects BGP routing information from various locations on the globe. The historical BGP data between the first time Root Servers used IPv6 in the beginning of 2008 and June 1st 2016 is studied. The evolution of IPv4 and IPv6 catchment areas of selected Root Servers over the time period is analyzed and then specifically the differences between them are studied. Finally, a visualization tool to help operator assessing their IPv4/IPv6 catchment areas is also developed.

1.1. Goals

The goal of this thesis is to assess the differences between IPv4 and IPv6 catchment areas of an anycasted services, with DNS Root Servers as the case study. Therefore, the following main research question (RQ) is used:

RQ: How different is IPv4 and IPv6 catchment areas of DNS Root Servers?

In order to address the main RQ, we define four sub RQs as the following:

RQ.1 ***How can we measure the control plane of anycast DNS system?*** There are several methodologies of anycast measurement found in the literature during the last 15 years. Some relevant measurement projects are also present today. Those are discussed to find the most appropriate one for this thesis.

RQ.2 ***How do IPv4 and IPv6 catchment areas evolve over the time?*** With the booming of the Internet, IP networks in general are constantly expanding. Infrastructures are continuously being deployed and network interconnections between organizations are being made. This results in the dynamics of Root Server' anycast networks over the time as well.

RQ.3 ***How different is IPv4 and IPv6 catchment areas?*** IPv6 networks are built years after IPv4 ones, and not as vast as its predecessor yet. It is interesting to find out to what extent the difference is from control-plane perspective.

RQ.4 ***How to represent the knowledge to the operator?*** Visualization is the best method to represent the knowledge of the networks, so that the operator may easily assess the IPv4 and IPv6 catchment areas of their anycast service.

1.2. Structure

This thesis is organized as follows. Chapter 2 provides related background knowledge of this thesis and state-of-the-art of anycast measurement, especially from control-plane perspective. It provides partial answer for RQ.1. Chapter 3 explains about our methodology and considerations used in this thesis. It provides the final part for RQ.1

answer. Chapter 4 discusses about the result of this work. It provides the answers for RQ.2, RQ.3, and RQ.4. Finally, Chapter 5 concludes this thesis by providing the concluding remarks and future works.

2. Background

This chapter discusses relevant topics to this thesis and state-of-the-art of anycast measurements. It is started with the concept of DNS (Section 2.1) and IP anycast (Section 2.2). Next, methodologies used for anycast DNS measurements as described in the literature are discussed in Section 2.3. Subsequently, the measurement of catchment areas from control-plane perspective is described in Section 2.4. Then, state-of-the-art of anycast visualization is discussed in Section 2.5. Section 2.6 provides the concluding remarks of this chapter.

2.1. DNS

As described in RFC 1034 [45], *Domain Name System* (DNS) is a distributed database system that essentially provides mapping between IP address and the corresponding name, and vice versa. The data for the mapping is stored in an inverted-tree-structured distributed database (Figure 2.1), where each node is called *domain*. The topmost level of the hierarchy is called the *root domain*, represented by a single dot ('.'), and becomes the starting point of a query. The next level consists of *top-level domains* (TLDs), *e.g.*, `.com`, `.net`, `.id`, and so on. Each domain becomes the root of a new *subdomain*. Every domain has a unique name, called *fully-qualified domain name* (FQDN), which is the sequence of labels from the node at the root of the domain to the root domain. Each domain can be divided further into *subdomains*, and responsibility for each subdomain can be delegated to a different organization.

The DNS has three major components [45]:

The domain name space and resource records A domain name [46] identifies a node, and the goal of domain names is to provide a mechanism for naming resources (re-corded as *resource records*, RRs) in such a way that the names are usable in different hosts, networks, protocol families, and administrative organizations.

Nameservers Nameservers manage two types of data. Firstly, it maintains *zones*, where each zone is the complete database for a particular segment of domain space (called authoritative). Secondly, it keeps *cached data* acquired by local resolvers, and used to improve the performance of query process when non-local data is frequently accessed. Nameservers also have pointers to other name servers that can be used to lead to information from any part of the domain tree.

Resolvers The local agent that accesses nameservers due to query requests from clients. It handles a nameserver queries, response interpretation, and returning the information to the requesting clients.

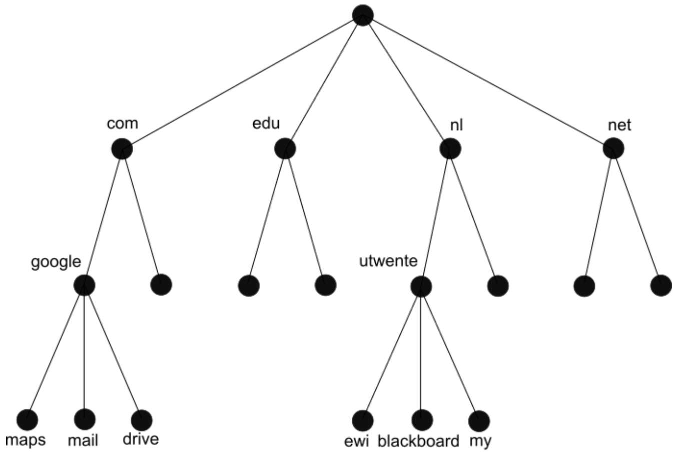


Figure 2.1.: Example of DNS database tree

Root nameservers, shortly called *Root Servers*, is the nameservers for root zone. It contains information of the authoritative nameservers for each of TLD zones. Any DNS queries, except for queries in the authoritative list of a nameserver, requires a response from a root server to be answered (and the answer can be cached for some determined time).

Root Servers role is critical in DNS because they are needed for the first step of DNS translation. Without them, the DNS simply does not work. Considering that DNS becomes one of the fundamental protocol in Internet infrastructure, failure in DNS may results in major broken connectivities. Currently, there are 13 Root Servers in the world (named from `A` to `M`) managed by different organizations, with the names in the form of `<alphabet>.root-servers.net`. The comprehensive information about Root Servers and their distributions around the world are available in [55].

2.2. IP Anycast

RFC 1546 [50] describes IP anycast as a technique to share IP address in common among multiple nodes in multiple locations relying on the BGP routing to map clients to anycast nodes (*one-to-any* connection). Figure 2.2 illustrates conceptual anycast. A client (red node) sends datagrams towards an anycast address, which is assigned to a group of nodes (green ones). The routing scheme on the network will deliver the datagrams towards *one* of the green nodes which satisfies the best-fit requirement (typically the shortest topological distance). Anycast is intended for services where the users are only care about the service delivery, regardless which server provides it.

There is also another type of anycast, called *application-layer anycast* [12]. As the name implies, it works at the application layer. In contrast, IP anycast works in network

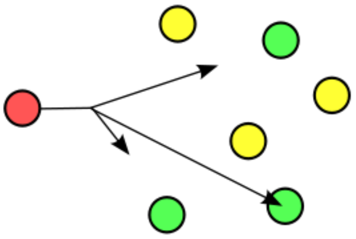


Figure 2.2.: Illustration of anycast (copied from [5])

layer. This thesis focuses on IP anycast only. For the rest of this report, *IP anycast* and *anycast* are used interchangeably.

The use of anycast in DNS operation was initially motivated by a DDoS attack targeting all DNS root servers on October 21st 2002. The attack [60], which congested the Root Server's upstream link, caused 9 out of 13 Root Servers to be unreachable. This resulted, among others, in anycasting the Root Servers. A number of Root Servers' instances configured with the same IP address are spread to different locations across the globe. Therefore, if another attack hits a Root Server's node, the other servers in different locations remain operational, and service disruption can be localized. This approach proved to be effective when on February 6th 2007 another DDoS attack launched against at least 6 Root Servers, and only two of them were noticeably affected because those were not anycasted yet [28]. As the result, up to 72% TLD servers are anycasted in 2013 [29], and today all Root Server–except B and H–implement anycast [55].

On the other hand, DNS protocol itself perfectly matches anycast characteristics. Most of DNS communication occurs over either single datagrams or short-lived TCP flows. It fits IP anycast narrative which forwards on per-datagram basis. Implementing anycast in DNS operation is beneficial for the following reasons [21, 2]:

Resilience. As explained before, by anycasting the servers and spread the servers on multiple locations globally, the attack load are localized, hence the users in that area can be served by other anycast nodes unaffected by the attack. If the server is not responding, the router can be reconfigured to withdraw the prefix announcement from that area.

Performance. Deploying nodes topologically close to clients is expected to decrease query times. In addition, distributing nameservers across the globe will help spreading query traffic from users as well, thus reducing loads per server. This is especially useful for root and TLD nameservers which become the center of DNS operations and experience high load of traffic.

Reliability. Deploying nodes closer to clients in different regions decrease the number of hops that DNS queries must traverse, hence reducing the chance of network failure.

Simplicity. Anycast allows operators to reduce a list of service addresses for each instance to just a single distributed address.

As explained before, anycast service uses a single address. In global routing (BGP), this address is represented as an address prefix. Based on how the anycast prefix is announced from the anycasted service to the upstream BGP, anycast node can be categorized into *local* and *global* node. The former one is intended to serve only a limited area, while the latter one is to serve the entire Internet. Local nodes are typically configured using BGP `NO_EXPORT` or `NOPEER` flags, so that the BGP peers receiving the anycast prefix advertisements does not forward further. Global nodes path announcement does not use such flags, and is artificially lengthened using AS-path prepending to affect BGP route selection. RFC 4786 [2] provides detailed guidelines over anycast service deployment within routing systems. The deployment configuration which contains both local and global nodes is said to be *hierarchical*, while if all nodes are globally visible, then it is said to be *flat*.

The topological region of a network within which packets from users directed at an anycast address are routed to one particular node is called *anycast catchment* [2]. The catchment area is typically defined by the mapping user-to-node that BGP makes. If there is BGP misconfiguration for local node advertisement such as prefix leaking, the catchment will likely be beyond the intended area and may result in non-optimal node selection.

There are three methods used by Root Server operators to announce anycast prefixes[1]: *(i)* operator may use a single AS as the origin AS of the anycast prefixes from all of their instances that directly connected to its BGP peers. *(ii)* Each global instance announces the prefixes from a unique origin AS, as recommended by RFC 6382 [24]. *(iii)* All instances announce the prefix from a single origin AS, and there is a unique local AS for each instance intentionally put between the origin AS and the peers that used as the physical identifier of the instance at AS-level.

The first method is intended to preserve ASN needed and to ease management overhead, including to prevent inconsistent origin AS problem[2]. Most Root Servers implement this technique. As described in [24], The second method aims to better detect changes to routing information associated globally anycasted services and for security reasons. The downsides are only organizations with numerous ASNs are able to do it, and that the anycast prefixes will regularly appear in inconsistent origin AS report. A and J-Root use this in practice. The last one is regarded as the compromise between two former methods. It is intended to preserve the inconsistent-origin ASN reports while at the same time to provide instance identification at network-level. The third

[1] The upcoming descriptions contain several concepts in BGP, which are explained in Subsection 2.4

[2] A problem where single prefix is originated by multiple ASes. Generally, it is used as an indication of prefix hijack, where a prefix is announced by an unauthorized AS to withdraw traffic to it

method is employed by ISC, the operator of F-Root.

2.3. Anycast Measurement

Recall that anycast is a distributed service. Thus, it also requires distributed probes as user representations to perform measurements. In general, active measurements are performed mainly by sending `ping`, `traceroute`, or DNS queries towards anycast instances in regular basis. Passive measurements are typically conducted by analyzing the incoming packet traces or server logs. It can also be done by analyzing routing system information, such as BGP routing table.

Table 2.1 summarizes measurement methodologies for anycast DNS used in literature for the last 15 years. Latency measurement is performed to get the degree of server proximity from the round-trip time (RTT). Service availability is measured via responses from regular DNS queries. Then, since users cannot determine which instance to serve them, instance identification is performed by sending DNS query of `CHAOS.TXT` for `HOSTNAME.BIND` [62]. Regular instance identification can further be used to detect serving instance switches (happens due to service outage or network changes). Instance switch can also be performed at server-side by analyzing presence of users' address in all instance logs. To reveal the traversed paths, classic tool `traceroute` or AS path from BGP routing table can be used.

Latency measurement	
ICMP ping	[21, 17, 19, 18, 38, 20]
query response time	[37, 57, 21, 7, 41, 3]
traceroute	[63, 44]
Availability	
Via responses from DNS query	[37, 57, 41]
Instance discovery	
`CHAOS TXT` or `HOSTNAME.BIND` query	[21, 33, 30, 63, 29, 38, 20, 3]
Instance switches	
Server-side measurement	[8, 21]
Client-side measurement	[37, 13, 57, 33, 7]
Traversed path	
Traceroute	[30, 63, 44]
BGP	[13, 7, 42, 31, 43, 63, 44]
Service metrics	
Packet trace	[42, 43, 26, 17]
Server log analysis	[15]

Table 2.1.: Classification of measurement methodologies in the literature

In this thesis, we are in particular interested on the path revelation methodologies. Path revelation allows us to reveal anycast catchment areas. It shows reachability and connectivity of a service. `Traceroute` provides finer granularity compared to BGP's AS path, since it reveals all routers traversed along the path. `Traceroute` is simple to use, and it reflects the real path used by the service packets as it works on *data-plane* (part of the network that carries user traffic). However, it only provides a constrained view of the routing system and suffers from ambiguous results such as incomplete paths due to ICMP filtering along the paths. In contrast, BGP only provides a high-level view of connectivities at AS-level, since it works on *control-plane* (part of the network that makes the routing decision). However, it provides more complete view of the routing system; not only the end-to-end AS-level path from users to the anycast service provider, but also route information towards other ASes as well. In the next section, measurements using BGP routing tables and updates is discussed in depth.

2.4. Measuring IPv4 and IPv6 Catchment Areas from Control-Plane Perspective

The 32-bit IPv4 has been used as the device identifier in the network since the beginning of the Internet, and today we are running out of available IPv4 address space [3]. IPv6 is intended to provide much larger address space (128-bit) compared to IPv4 (32-bit) with other advantages as well, such as better security, mobility support, and simplification of network configuration. However, even after its standardization 20 years ago, IPv6 adoption is relatively slow. Study from [23] reveals that the number of IPv6 prefixes advertised in BGP has been increasing 37-fold between 2004 and 2014, compared to four-fold of IPv4. Nevertheless, the difference is almost two magnitude. Today, the figures have not changed that much, where the advertised IPv6 prefixes is just 0.0507 of IPv4[4].

Nikkhah et al. [47] categorized three major phases of IPv6 adoption: **(i)** *stagnation* (1995-2009) due to lack maturity of IPv6 initial version and sufficient IPv4 addresses available, **(ii)** *emergence* (2009-2012) due to growing incentive to adopt IPv6 and IPv6 quality improvements, and **(iii)** *acceleration* (2012-), due to IPv4 addresses exhaustion and sufficient IPv6 adoption at the core Internet to ensure quality of IPv6 connection is equal with IPv4. They also demonstrated that prior to 2011, IPv6 performance gap was largely due to its data-plane (*e.g.*, poor hardware/software performances). Starting from 2011, IPv6 was finally equivalent with IPv4 technology-wise and the gap is primarily due to control-plane performance. Often cases where IPv4 and IPv6 paths are different primarily because of adoption decisions. Instead of following the optimized IPv4 path, IPv6 routing is required to travel around routing domains that have

[3] `http://www.potaroo.net/tools/ipv4/`

[4] `http://bgp.potaroo.net/v6/v6rpt.html`, accessed on August 6th 2016

either not deployed IPv6 yet or chose not to establish IPv6 peering sessions with their neighbors.

The discrepancy between IPv4 and IPv6 paths are crucial since it could affect the service quality. Dhamdhere et al. [27] showed that if the AS-level path was the same in both protocols, performance over IPv6 paths is comparable to that over IPv4. However, it can be much worse than IPv4 if the AS paths differ. This is especially important for anycast DNS, since AS path difference could lead to different physical instances as well. Geographically further anycast node results in longer response time, which could degrade the quality of service. Since many protocols relied on DNS to work properly (*e.g.*, e-mail, web, CDN), the overall service quality could get worse as well.

Therefore, besides performing typical data-plane measurements to assess the service, monitoring IPv4 and IPv6 catchment areas at control-plane level is also important. Before control-plane-based measurement is discussed, the concept of BGP is briefly explained first.

Autonomous System (AS) is a region in the Internet which is under a single administrative control, and is identified by a globally unique AS number (ASN) allocated by Regional Internet Registries (RIR). BGP [1] itself is the *de-facto* inter-AS routing protocol. It is primarily used to exchange network reachability information at IP address prefixes level (referred as *prefixes*) with other BGP systems by making routing decisions based on paths, network policies, or pre-configured rule-sets. AS that announce the presence of a prefix is referred as *origin AS*. In order to get connected with other ASes, an AS may choose to use *transit* service from larger ISP called *upstream provider*, or it may decide to directly interconnect with other AS (*direct peering*). The policies determine which route to choose and to be propagated to the peers. it is largely defined based on the business relationship of the operators. For example, traffic over customers is preferred than over other providers, since it generates more revenue. On the other hand, traffic via direct peering is favored over transit since it minimizes the cost. These factors, among others, are often lead to sub-optimal BGP routing.

A BGP router maintains network reachability information in the *Routing Information Base* (RIB). RIB consists of three parts (Figure 2.3): *(i)* `Adj-RIBs-In` (unprocessed routing information learned from inbound Update messages received from other BGP speakers), *(ii)* `Loc-RIB` (local routing information selected by applying local policies to the routing information contained in `Adj-RIBs-In`), and *(iii)* `Adj-RIBs-Out` (stores information to be advertised to peers).

An anycast service, which is essentially a subset of the Internet itself, is identified at network level through its announced prefixes. The anycast prefixes is part of BGP's network reachability information. To understand and analyze how the anycast catchment works at global Internet, the routing protocol running it–*i.e.*, BGP–should be used as the reference. However, BGP is a complex protocol, especially due to the pres-

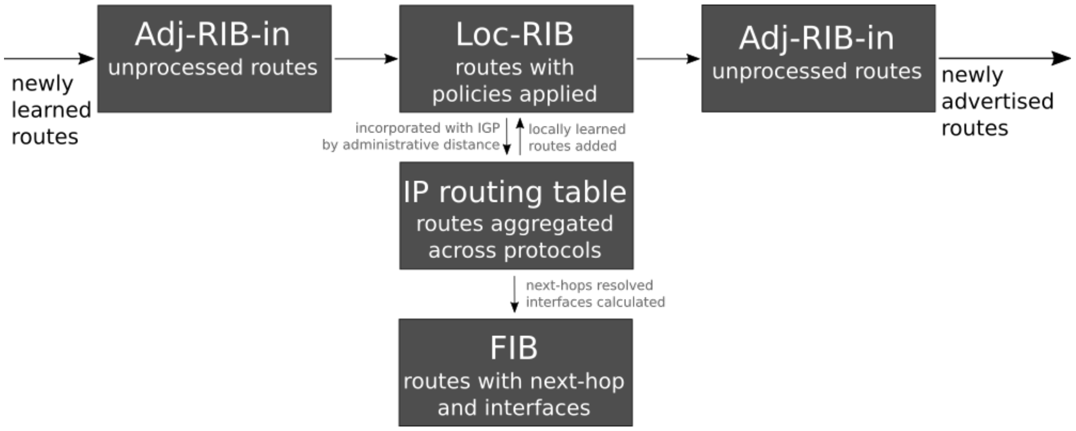

Adj-RIB-in
unprocessed routes
newly learned routes
Loc-RIB
routes with policies applied
incorporated with IGP by administrative distance
locally learned routes added
Adj-RIB-in
unprocessed routes
newly advertised routes
IP routing table
routes aggregated across protocols
next-hops resolved interfaces calculated
FIB
routes with next-hop and interfaces

Figure 2.3.: BGP update process (reproduced from [34])

ence of different routing policies implemented by participating organizations. One router may have different BGP route toward a specific destination compared to others, and each router has limited view of the Internet topology. Therefore, gaining knowledge of global Internet only from a single BGP router is definitely not sufficient.

There are three methods available to get BGP routing information from multiple routers: *(i)* using looking glass, *(ii)* collecting BGP routing information by establishing a BGP peering session with routers using collectors, and *(iii)* using BGP monitoring protocol such as BMP. The summary of these methods including well-known monitoring projects using it is presented in Table 2.2.

Looking glass is a web-based application managed by operators to provide a view into the BGP routing tables of their BGP routers. It is basically an interface to execute limited range of commands inside the routers. It provides real-time information of the BGP state of a router with no possibility to access historical data. Therefore, looking glass is more appropriate for troubleshooting purposes.

The second method is by deploying BGP route collectors at various Internet exchange points (IXP) in the world. Route collector, simply referred as *collector*, is a host running a collector processes (such as Quagga[5]) which emulates a router and establishes BGP peering sessions with one or more participating routers (referred as *peers*). Each peer sends BGP Update messages to the collector each time the `Adj-RIB-out` changes, which reflecting changes to its `Loc-RIB`. For each peer, the collector maintains `adj-RIB-out` table built based on BGP Updates received. The collector periodically dumps the maintained `Adj-RIB-out` (*RIB dump*) and the BGP Update messages (*Update dump*) received from all of its peers since the last dump. Typically, the dump frequencies are few hours for RIB and few minutes for Updates (see Table 2.2). This data dump is then archived in MRT Routing Information Export [40] format.

[5] http://www.nongnu.org/quagga/

	Start	Managing Organization	Collecting Method	Data Accessibility	Collector Locations	Dump Frequency	Histor-ical	(Near) Real-Time	Note
Looking glass	-	Network providers	accessing router's RIB	web interface	-	-	✗	✓	real-time BGP state
RIS [53]	2001	RIPE NCC	route collectors	MRT file, REST API	Europe, USA, Brazil, Japan, South Africa	RIB 8 hours, Update 5 min.	✓	✗	REST API via RIPEStat
RouteViews [59]	1997	University of Oregon	route collectors	MRT file, XML stream	USA, UK, Serbia, Kenya, South Africa, Australia, Nepal, Japan, Brazil	RIB 2 hours, Update 15 min.	✓	✓	live stream is accessed using BGPMon
BGPMon [11]	2008	Colorado State University	route collectors	XML stream	uses RouteViews collectors	-	✓	✓	archives accessed in MRT and bgpdump formats
PCH [49]	2010	PCH	route collectors	MRT file, routing table overview	100+ IXPs (details not available)	routing table snapshot daily, Update 1 min.	✓	✗	VPs are only PCH peers
Caida OpenBMP [14]	June 2016	Caida & RouteViews	BMP	Stream	uses RouteViews collectors	RIB 1 hour, Update 1 min.	✓	✓	Still in experimental phase

Table 2.2.: BGP monitoring methods

There are two well-known global monitoring projects that use this method in large scale, namely RIPE RIS [53] and RouteViews [59]. Both projects have been starting collecting BGP routing information from various locations and peers since the end of 1990s and make the archives available for public access[6][7]. In fact, both repositories become the main data sources used by researchers to study various subjects, such as routing policies, Internet topologies, security, and so on. The main issue with them is their file-based distribution system and the delay due to dump interval to make the data available. To analyze a certain prefix, for example, user is required to download the dump file of time interval in interest (can be very large in size) which contains data of other prefixes as well. Performing analysis of wide-range time period would require huge amount of storage and bandwidth to download the data. Fortunately, RIPE NCC as the operator of RIS develop RIPEStat [54], a web-based interface that provides access to any specific resources contained in RIS archives through its REST API. It allows user to access specific routing resource data (*e.g.*, prefix, ASN) in a fast and convenient way.

Other similar projects also exist. Firstly, PCH [49] provides their BGP routing data accessible for public as well. However, instead of providing the RIB dump, they only provide snapshot of BGP routing table overview from the output command of '`show ip bgp`'. Furthermore, judging from its dump size that relatively small compared to RIS or RouteViews, we believe that its route collectors only gather information from PCH peers (not from participating organizations such as RIS or RouteViews). Second project is BGPMon [11], a distributed BGP monitoring system that provides real-time data stream in XML format for both BGP updates and RIB snapshot. It uses streamlined collectors that allows it to be more scalable on handling large number of peers. Initially, BGPMon used its own infrastructure to perform measurement. Today, it is used by RouteViews to replace Quagga as the collectors and allows RouteViews to provide live feeds. Unfortunately, BGPMon does not provide historical data access in the same way as its live stream. It stores BGP data in MRT and bgpdump formats hence retains the same issue of file-based distribution.

There are limitations with the use of BGP route information from collectors [56, 32]:

1. The type of information that can be collected is not always the same. Most updates from collectors' peers are *full-feed* (contains the entire `Loc-RIB`). However, some updates are *partial-feeds* (only a subset of its `Loc-RIB`) which may go through a filtering process before being sent to the collectors.
2. The collector can only see what the connected router advertises. It cannot access what BGP updates a peer receives from its neighbors (peers of a peer). To get all routes, the only way is to examine the BGP `Adj-RIB-In` for each peer.
3. some ASes are very large geographically, thus the view in each geographical

[6] http://archive.routeviews.org/

[7] https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data

region might be different for each router in that AS.

4. The number of collectors available are quite limited, and its placement is geographically and topologically biased. The first bias especially happens in RIS, where most of its collectors reside in Europe. Second bias comes from the fact that the collectors receive data from volunteer networks that mostly are large top-tier ISPs. Therefore, many peer-to-peer connections that may be established among ASes at the Internet edges may not detected. The number of ASes that feeding the collectors are also quite small compared to the total advertised ASes on the Internet. Thus, it results in extremely narrow view of the Internet.
5. The connections between collectors and routers are not reliable all the time. Data loss might occur anytime.

The third method is an attempt to improve some shortcomings above using *BGP Monitoring Protocol* (BMP) [36]. BMP is used to monitor BGP sessions, and the primary improvement over traditional BGP peering method is the capability to access `adj-RIB-in` to get complete dump of the routes received by a peer (including routes from peers of a peer). Instead of using collector, the participating peers connects to a management station, sends initial dump of all routes for those peers. As peers advertise or withdraw routes, additional updates are sent to the management station. Thus, user is not required to wait until the data dump available. OpenBMP [48] is an open-source implementation of BMP and supported by the latest Cisco and Juniper's OS. It allows to periodically access the `adj-RIB-in` of a router or to monitor its BGP peering sessions.

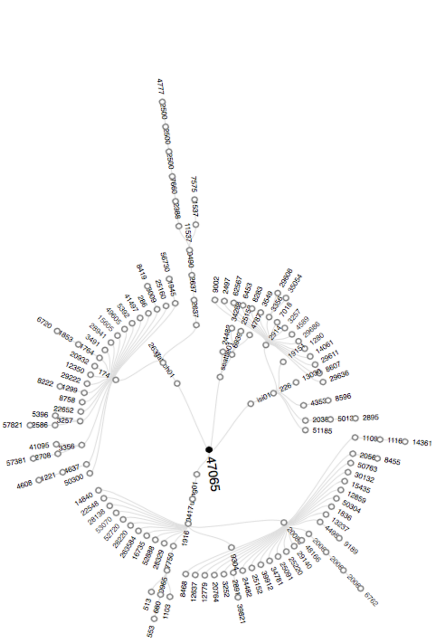
Despite of its promising improvement, unfortunately there is no large-scale project yet that provide their BMP data publicly as RouteViews or RIS do. An experimental project conducted by Caida and RouteViews [14] to use OpenBMP on RouteViews collectors is underway to allow real-time and historical data access, which might be available for public in the near future. Therefore, despite of its imperfectness, RIS and RouteViews still provide the largest usable BGP routing datasets.

2.5. Anycast Visualization

BGP route visualization belongs to the domain of graph drawing, which follows theory rules covered by graph theory. It is a visual representation of the vertices (link between ASes) and edges (ASes). Control-plane Anycast visualization itself can be performed using typical methods for BGP visualization.

There are several related works on visualizing BGP topology. Since 2000, CAIDA has generated *AS core graphs* (also referred as AS-level Internet graphs) representing a macroscopic snapshot of IPv4 and IPv6 Internet topology samples in order to visualize the shifting topology of the Internet over time, both for IPv4 and IPv6 [35]. It ranks ASes based on their transit degree; the higher the degree the more centered is the AS placement in the graph. Inspired by CAIDA's work, APNIC developed VizAS [61] to provide visualization of the BGP peering relationships within a single economy (e.g., a country). It shows two side-by-side IPv4 and IPv6 charts representing the visible autonomous network in the selected economy.

BGPlay [9] is a Java-based tool which displays animated graphs of the routing activity of a certain prefix within a specified interval to visualize the behavior and instabilities of of Internet routing at the AS level. It is fed using relevant BGP update messages for the specified time interval. BGPlay was used by Karrenberg [37] to visualize path changes between instances and probes in his study. To improve its portability, there is a work to implement BGPlay in pure JavaScript, called BGPlay.js [10], which uses routing data in a specified JSON format. It is currently being used in RIPEstat [54].



(a) Control plane - before

(b) Control plane - after

Figure 2.4.: Visualization of routing impact of adding or removing anycast instances, copied from [58]

Specific to anycast visualization, the authors of [58] proposed visualization tool for IP anycast to understand routing impact of adding or removing instances. Since BGP paths consist of a number of AS hops, it would be easier to understand if ASes with the same hop degree relative to the measured AS are grouped together. Thus, they use radial tree graph based on the Reingold-Tilford algorithm [52] for efficient, tidy arrangement of layered nodes. They use PEERING platform [51] as the anycast testbed consisting of 7 instances spread in USA, Brazil, and the Netherlands. They use a subset of RIPE Atlas probes that periodically run `traceroute` towards PEERING. The BGP routing data is collected from both `traceroute` and RIS collectors. The tool separates the view into two segments: control and data planes. Control plane visualization is used to see the changes in BGP routes when there is a change (withdrawal or announcement) of an instance. The data is taken from RIPE RRC. In order to quantify changes take place in data plane, a periodic traceroute measurements are performed using RIPE Atlas probes. The result of their visualization for control plane is presented in Figure 2.4. It shows the anycast catchment areas before and after the instance announcement. The ASes are arranged in a hierarchy based on the degree towards the origin AS.

To summarize, CAIDA's graph and VizAS are impressive. They are intended to visualize high-level overview of the topology by focusing more on who are the big players in the networks. Since the diameter of the outer circle is fixed, as the networks become larger with huge numbers of edge ASes then the graph becomes difficult to read due to denser outer circle. BGPlay excels at visualizing AS-level network changes over a period of time. As it visualizes every BGP Update message events, it provides very detailed information. Thus, BGPlay is more suitable as troubleshooting tool. Result from [58] is the closest to the requirement of this work. Improvements can be made, especially in the interactivity part.

2.6. Concluding Remarks

`Traceroute` and BGP routing information are the two methods used by literature to reveal anycast catchment areas. Despite of its simplicity and finer granularity, `traceroute` suffers from ICMP filtering often implemented along the path. On the other hand, BGP routing data provides high-level view of connectivity, but reveals end-to-end AS-level paths. For this study, using BGP routing data is more appropriate as we need broad view of the networks to understand the catchment areas. In order to obtain historical BGP routing data, using public data from measurement projects such as RIS and RouteViews is preferred over other approaches. Finally, to visualize comparison of IPv4 and IPv6 anycast catchment area, work in [58] is the closest to this work, and thus it can be developed further to fit our requirements and to include interactivity features.

3. Methodology

This chapter discusses methodology used in this study. Firstly, the selection of Root Servers used is presented in Section 3.1. Secondly, the method used to retrieve historical BGP data is discussed in Section 3.2. Thirdly, types of data analysis performed and considerations taken is presented in Section 3.3. Fourthly, visualization technique we used in Section 3.4. Finally, the concluding remarks of this chapter is provided in Section 3.5.

3.1. Selecting Eligible Root Servers

As discussed in Section 2.1, there are 13 Root Servers in operation today. However, not all of them are eligible for this study. The objective of this thesis is to assess IPv4/IPv6 catchment areas of anycast service. Thus, we only select Root Servers that are anycasted and provide dual-stacked services. Among all Root Servers, we omit B and H-Root as these Roots are not anycasted yet. We also rule out E and G-Root as those are IPv4 only. Thus, it leaves us with A, C, D, F, I, J, K, L, and M-Root.

Table 3.1 presents all Root Servers used in this study. The selected Root Servers have different starting date of dual-stack operation. Since the majority of them (A, F, H, J, K, M) started using IPv6 from February 2008[1], the data analysis is started from March 1st 2008 and ended on June 1st 2016. The other Root Servers (C, D, I) started using IPv6 later. We cannot find information regarding L-Root's starting date. However, based on the BGP routing data, it seems L-Root started to run dual-stacked service at least in February 2008.

Root Servers use single address for each IPv4 and IPv6 for their DNS service. However, some of them changed their addresses during the observation time (second column of Table 3.1). These changes are taken into account as well in our analysis program.

3.2. BGP Data Retrieval

As discussed in Section 2.3, there are two projects that provide large-scale historical BGP routing data, namely RIS and RouteViews. Looking at their collector list, RouteViews[2] has advantage over RIS (Table 3.2) in terms of collectors distribution. RIS is

[1] http://www.iana.org/reports/2008/root-aaaa-announcement.html

[2] http://archive.routeviews.org/

Root Server	IP Addresses	IPv6 Starting Date[a]
A	198.41.0.4 2001:503:ba3e::2:30	Feb 2008
C	192.33.4.12 2001:500:2::c	Mar 2014
D	128.8.10.90, 199.7.91.13[b] 2001:500:2d::d	Mar 2014
F	192.5.5.241 2001:500:2f::f	Feb 2008
I	192.36.148.17 2001:7fe::53	Jun 2010
J	192.58.128.30 2001:503:c27::2:30	Feb 2008
K	193.0.14.129 2001:7fd::1	Feb 2008
L	198.32.64.12, 199.7.83.42[c] 2001:500:3::42, 2001:500:9f::42[d]	N/A
M	202.12.27.33 2001:dc3::35	Feb 2008

[a] http://www.root-servers.org/news.html
[b] Switched to the second IP address in January 2013
[c] Switched to the second IP address in March 2016
[d] Switched to the second IP address in November 2011

Table 3.1.: Root Servers used in this thesis

Europe-centric, where only 6 out of 18 collectors are outside the continent and 3 of them are in USA. On the other hand, RouteViews is more globally distributed. Beyond the US and European countries, RouteViews also deploy collectors in Australia, Singapore, Nepal, and Kenya. Using both data source would be complementary. However, RouteViews only provides the raw MRT files. Typically, each collector produce ~100 MB of BGP RIB data for each dump interval that its size keeps growing over the time. Suppose there are 17 collectors. Thus, for the time period used in this thesis (each month between March 2008 and June 2016), we should download 17×100 MB $\times 88$ months $= 149.6$ GB, not including time required to process the raw data. Due to time and resource constraints in this work, using data from RouteViews is considered to be not feasible.

On the other hand, RIS collectors data can be accessed through RIPEStat using its API, which allows us to only access specific BGP routing information that we need. Thus, we use RIPEStat as our data provider. We specifically need to access reachability of all RIS collectors' peers in the form of AS paths to a certain prefixes, *i.e.*, the Root Servers' prefixes, at a point of time. To do this, we employ data call "BGP State"[3]. We use the

[3] https://stat.ripe.net/docs/data_api#BGPState

Code	Location	Operating Date
rrc00	RIPE NCC, Amsterdam	Oct 1999
rrc01	LINX, London	Jul 2000
rrc03	AMS-IX and NL-IX, Amsterdam	Jan 2001
rrc04	CIXP, Geneva	Apr 2001
rrc05	VIX, Vienna	Jun 2001
rrc06	Otemachi, Japan	Aug 2001
rrc07	Stockholm, Sweden	Apr 2002
rrc10	Milan, Italy	Nov 2003
rrc11	New York (NY), USA	Feb 2004
rrc12	Frankfurt, Germany	Jul 2004
rrc13	Moscow, Russia	Apr 2005
rrc14	Palo Alto, USA	Dec 2004
rrc15	Sao Paulo, Brazil	Dec 2005
rrc16	Miami, USA	Feb 2008
rrc18	CATNIX, Barcelona	Nov 2015
rrc19	NAP Africa JB, Johannesburg	Nov 2015
rrc20	SwissIX, Zurich	Nov 2015
rrc21	France-IX, Paris	Nov 2015

Table 3.2.: List of RIS collectors used in this study

IP address of a Root Server as the argument, instead of its prefix. This is because some operators prefer to announce different anycast prefix lengths to distinguish global and local catchments. For instance, F-Root uses /23 prefix for its global nodes and /24 for local instances, so that routers which possess both routing information will prefer the local instances (if present) as its prefix is more specific. By using Root Server's IP addresses, we hand over the decision of which prefix chosen by the RIS peers for those addresses to the system. For example, to query BGP routing data for IPv4 prefix of M-Root on June 1st 2016, then the following URL is used. Here the date is converted into UNIX timestamp:

`https://stat.ripe.net/data/bgp-state/data.json?resource=202.12.27.33&timestamp=1464739200`

RIPE RIS collectors gather BGP information from participating routers. These peers act as *vantage points* or VPs for our measurement, and from now on we refer them simply as *VPs*. VPs may have IPv4 and/or IPv6 route information towards certain Root Server. Those that possess routes to both IPv4/IPv6 prefixes of a Root Server at a given time are referred as *dual-stacked VPs*. Dual-stacked VPs becomes the primary subject of this thesis since they allow us to perform comparable analysis of IPv4 and IPv6 catchments.

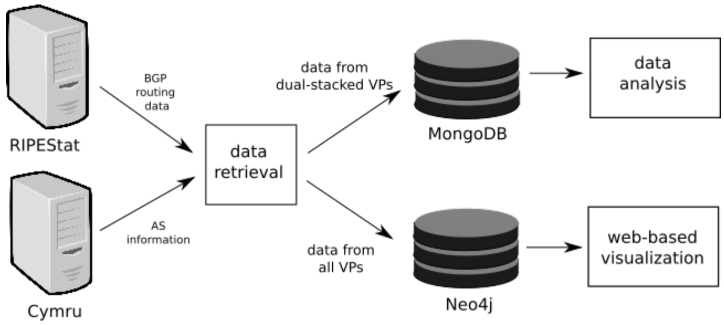


Figure 3.1.: Workflow of this study

It should be noted from Table 3.2 that the starting operation date among RIS collectors are different. This affects in the total number of the participating peers at a time. However, since the observation period is started in March 2008, the impact of new collectors addition only takes place starting in November 2015. This is particularly reflected in the notable increase of dual-stacked VPs of all Root Servers starting in the end of 2015, as can be seen later in the Chapter 4.

Figure 3.1 illustrates the workflow of this study. All BGP data related to Root Servers' prefixes between March 1st 2008 and June 1st 2016 for every first date of each month is retrieved from RIPEStat, and then persisted in two databases. Data from dual-stacked VPs that is used for data analysis is stored in MongoDB. MongoDB is selected because it is document-oriented and the data itself is in JSON format, hence makes the analysis process straightforward. Data from all VPs are stored in the second database, Neo4j, for visualization purpose. Neo4j is a graph database, hence it fits well with the nature of BGP. It makes the queries for visualization easier. All code and data used throughout this work, including the more detailed technical description, are available at our Github repository [4].

To make the visualization informative, short description of ASes is needed. Data provided by Team Cymru Research[4] is used, which is accessible through their WHOIS service. Initially, we chose to perform real-time WHOIS query to provide visualization interactivity. However, sometimes Cymru does not provide quick response, which leads to poor user experience. Therefore, we decided to download AS information for all unique ASes in the database, so that the visualization front-end can quickly retrieve the data from local database. We believe that this is justified because ASN does not change much, so it is safe to have a copy in local repository.

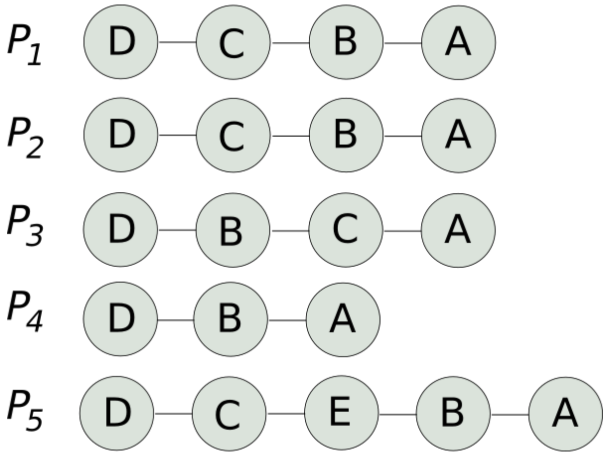


Figure 3.2.: Illustration of AS path definition

3.3. Data Analysis

The Internet can be modeled as graph, $G = (V, E)$. A vertex in V represents AS, and edges in E are peerings between ASes. An AS path between a source AS (*i.e.*, VP of RIS) A and destination AS B (*i.e.*, the origin AS of Root Server's prefixes) is defined as $P_{AB} = v_0 \rightarrow v_1 \rightarrow v_2 \rightarrow ... \rightarrow v_n$ where $v_0 = AS_A$, $v_n = AS_B$, and n denotes the hop number. In this thesis, we say that P_1 is identical to P_2 if $n_1 = n_2, v_{i1} = v_{i2}$ for $i \in [0, n]$. Otherwise, P_1 and P_2 are said to have different path. In the case of $n_1 \neq n_2$, we say that P_1 is shorter than P_2 if $n_1 < n_2$.

Figure 3.2 illustrates AS paths relationship definition above. All paths P_1 to P_5 have origin AS A and source AS D. P_1 is identical to P_2 since all of their transit ASes are identical. P_1 and P_3 are said to have different path even though the path lengths are similar, since there is a transit AS for a certain degree that does not identical for both of them. P_4 is said to have shorter path than P_1, and in contrary P_5 has longer path than P_1.

Networking communities use the term *peering* to refer BGP session between two networks to exchange traffic between each others, typically for free. The relationship is equal for both sides. Thus, they try to keep the traffic flowing in both directions to be balanced, so that they have bargaining position to keep the connection free. Otherwise, the other party will start to charge them if their traffic is higher than their counterpart. On the other hand, the term *transit* is used to describe paid BGP session between customer and provider where the provider carry all of their customer's traffic (inbound and outbound) to/from the Internet. Since it is difficult to infer the economic relationship between Root Server and their next-hop ASes based on the dataset we have, this thesis uses the term *peering* broadly as its basic meaning, which is the BGP

[4] http://www.team-cymru.org/index.html

session between two BGP speakers regardless the economic cost, to refer connection between Root Servers' origin ASes with their adjacent ASes.

In this thesis, we perform comparison on IPv4 and IPv6 AS paths of a VP. If a dual-stacked VP has identical IPv4 and IPv6 paths for certain Root Server's prefixes, we refer it as *converging VP*. If the paths are different, then we refer it as *diverging VP*. The amount of dual-stacked VPs and converging VPs of a Root Server at a given of time is an important metric used to determine the convergence level, as discussed later (Section 3.3.2).

To analyze the catchment areas, we address two subjects: *(i)* evolution of catchment areas (Section 3.3.1), and *(ii)* the difference between IPv4 and IPv6 catchment areas (Section 3.3.2).

3.3.1. Evolution of Catchment Areas

This subject is intended to understand the AS-level dynamics due to changes made by the operators on their networks over the time. In the context of this thesis, we focus to see the dynamics in two things: *(a)* the IPv4 and IPv6 networks becomes either divergent/convergent or intact, *(b)* the average path lengths over the time. Thus, we use all data from VPs that possess route information towards both IPv4 and IPv6 prefixes of the Root Servers (dual-stacked VPs).

Ideally, IPv4 and IPv6 catchment areas of a certain anycast service should be identical. In another word, IPv4 and IPv6 AS paths towards the anycast service from any given point in the Internet topology should follow the same AS hops. In this way, IPv4 and IPv6 users experience the same path from control-plane perspective. However, this does not always the case. There are factors leading to different IPv4 and IPv6 paths towards the same destination as experienced by VPs. Firstly, the deployment of IPv6 is not as mature as IPv4 network yet. There are still some parts in the Internet that only provide IPv4 routing capabilities, especially on the Internet edges. Secondly, the network operators may have different policies or peering agreements between IPv4 and IPv6 traffic with other operators. However, Dhamdhere et al. [27] suggests that the deployment of global IPv6 network are *converging* towards global IPv4 network. This can be easily understood since IPv4 network has been around for longer time and has been experiencing many optimizations and fixes of network misconfiguration, and can be considered as mature today. Thus, developing IPv6 networks based on IPv4 infrastructures will benefit from all lessons learned in the past.

To identify the convergence level of a certain anycast service (or service in general), we make use of AS path data from dual-stacked VPs. The fraction of converging VPs of all dual-stacked VPs at a time that see a Root Server's IPv4 and IPv6 prefixes is defined as the convergence level:

$$convergence\ level = \frac{\sum VP_{converging}}{\sum VP_{dual\ stacked}} \times 100\%$$

Another aspect from a catchment areas evolution we are interested at is to look at the trends of average path length over the time. The idea is to have shorter AS as possible between Root Server's origin AS and the users. While short paths does not automatically guarantee better user experience (it has to be verified at data-plane level), it generally shows that the distance between two parties are likely to be close. In case of shortest path possible (direct peering), it helps in many ways [16]: *(i)* it sidesteps potential obstacles in the form of additional transit ASes, *(ii)* it allows optimal use of BGP routing policy mechanism that usually do not propagate past one hop (MED, communities), *(iii)* possibility for joint traffic engineering, *(iv)* prevents spoofed traffic, *(v)* limits prefix hijacks, and *(vi)* speeds route convergence. To understand this in the context of DNS Root service, we calculate the distribution of dual-stacked VP path lengths over the observation period to see the trends.

3.3.2. The Differences Between IPv4 and IPv6 Catchment Areas

On the latter part, we focus on the differences itself as seen by the VPs. Thus, here we only use data from VPs that have different IPv4 and IPv6 paths toward a Root Server origin AS (diverging VPs). The diverging paths could happen because there are different routing policies applied for IPv4 and IPv6. For example, an operator may prefer to transit via provider *A* for IPv4 connectivities to the Internet and provider *B* for IPv6, perhaps due to some advantages offered by *B*. One particular case is Hurricane Electric, which offer free IPv6 peering[5]. In fact, diverging route is a common practice we found from the datasets. This convention may results in different IPv4 and IPv6 AS path lengths experienced by the diverging VPs.

There are three aspects discussed here. *Firstly*, the characterization of diverging VPs composition: how many of them experience shorter IPv4, shorter IPv6, and different paths but equal length. This information provides us illustration of an anycasted service's reachability level in IPv4 and IPv6. For example, does it really take care of its IPv6 users as its IPv4 ones? *Secondly*, the average path lengths is again studied. Only this time for diverging VPs. Hypothetically, longer AS paths have higher probability to have diverging paths, as it will traverse more intermediate ASes with potentially diverse routing policies, compared to the short one. Longer path also means that the source AS is more likely to be located at the edge of the Internet. As we know, the IPv6 deployment in Internet edges are still lagging. Thus, IPv6 route may take sidestep to

[5] although the traffic allowed to pass through is only for traffic with destination to Hurricane's network or its paid customers

round IPv4 only networks, resulting in longer path. *Thirdly*, we would like to know how different it is in terms of AS path lengths for diverging VPs.

3.4. Visualization

A tool is developed to visualize BGP path data obtained from RIPEStat. It is web-based, so that it can be easily accessed everywhere and integrated with existing monitoring tools. D3.js [25], a JavaScript library for manipulating documents based on data, is used at the front-end to render the graph due to its powerful and rich visualization types. To feed the visualization data, a back-end application based on Flask is developed, which accesses the databases described in Section 3.2.

The tool is developed based on work result from [58] (Section 2.5). One fundamental difference is the use of forced layout instead of radial Reingold-Tilford tree as used by the authors. While the latter one is excellent on arranging ASes based on their AS path level relative to the origin AS, it constructs the visualization based on each individual VP's AS path. Thus, the transit ASes might be visually duplicated in other part of the graph and does not provide complete picture of the catchment. Forced layout eliminates this by removing hierarchical display and provides visualization as a whole AS interconnections. To compensate the lack of AS path level information, we use color code to group ASes with the same AS path level. To simplify the visualization, AS prepending property is encoded as the thickness of the line connecting two ASes, instead of repeatedly displaying the same AS as sequence of nodes.

Further improvement is made by providing interactivity. Graph can be selected for any particular point of time in the observation period. To allow operator performing comparison, IPv4 and IPv6 catchment areas are displayed side by side with the list of mutual dual-stacked VPs presented below. As the network can grow quite large and complex, the graph elements can be zoomed in and out, panned, and moved for better readability. To make the IPv4/IPv6 path comparison of a certain dual-stacked VPs easier, both IPv4 and IPv6 AS paths are highlighted when it is hovered. The short AS description retrieved from Team Cymru is also displayed on top of it.

3.5. Concluding Remarks

Not all Root Servers can be used in this study because non-anycasted and IPv4-only are excluded. For the data provider, using both RIS and RouteViews would be complementary because they cover different collector placements. However, due to constraints in this work, only RIS is used since it provides easy access to their historical

BGP data. Then, some definitions used in the upcoming analysis is described in Section 3.3. The subjects of analysis are also presented, covering evolution of catchment areas and the differences between IPv4 and IPv6 catchments itself. Finally, for the visualization, we extend the work from [58] with a change graph type and improvements in visualization interactivity.

4. Result Analysis

The analysis of the work results is provided in this chapter. As described in Section 3.3, the analysis is divided into two topics: *(i)* evolution of catchment areas (Section 4.1), and *(ii)* the differences between IPv4 and IPv6 catchment areas (Section 4.2). The features of visualization tool intended to help operator assessing their catchment areas is discussed in Section 4.3. Finally, this chapter is concluded by a discussion about the importance of performing IPv4/IPv6 catchment areas for the operator in Section 4.4.

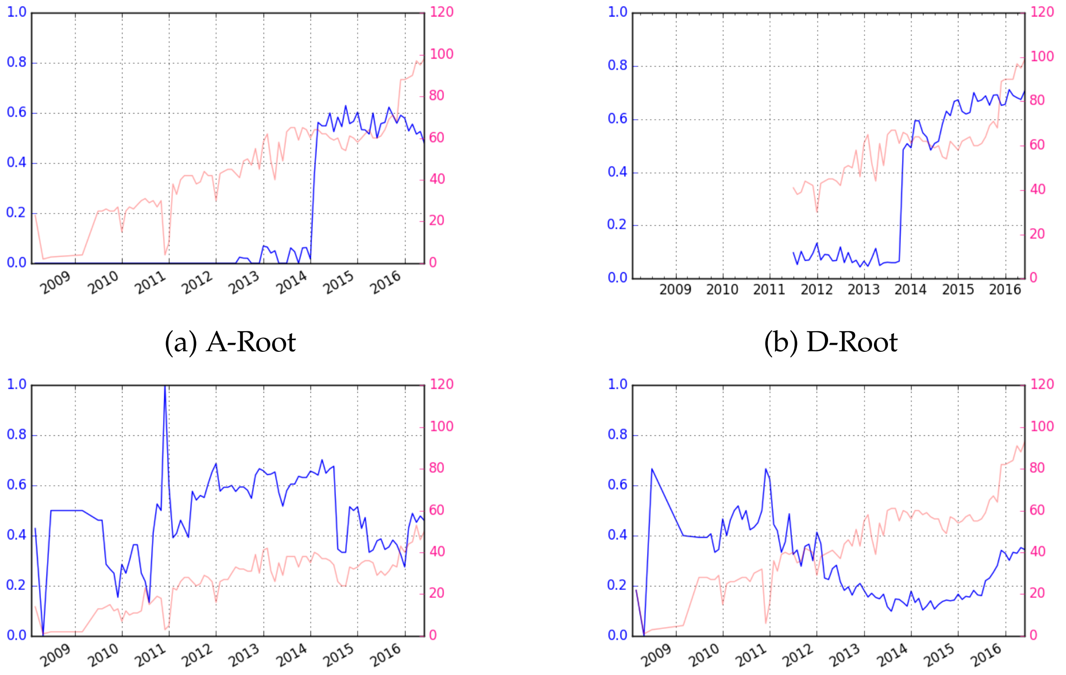
4.1. Evolution of Catchment Areas

Over the time, anycast operators may made changes on their network in order to improve the service. They may have added instances at underserved locations, changed their service policy, made new peering agreements with other organizations, and so on. These changes may result in congruity of the IPv4 and IPv6 catchments, or even higher differences between them. The changes may also not fundamental enough to change the catchment topology, hence it remains relatively the same throughout time. In this subsection, we discuss about the evolution of Root Server's catchment areas from control-plane perspective during the period March 1st 2008 to June 1st 2016.

4.1.1. Convergence

Recalling from Section 3.3.1, convergence level is a metric to describe the fraction of converging VPs of all dual-stacked VPs that see certain Root Server prefixes. Convergence levels of all Root Servers are presented in Appendix A, with some are presented in Figure 4.1. The blue line represents the convergence level, and the red line indicates the total number of dual-stacked VPs. The inclusion of the dual-stacked VPs into the graphs serves two purposes: *(i)* it can be used as the control when there is outlier data for convergence level. For example, K-Root (Figure A.1g) have convergence level 100% until the middle of 2009. By observing the number of VPs at the same time period, it is because there was only small number of VPs detected K-Root prefixes hence the skewed result. *(ii)* it can also be used to infer the visibility level of Root Servers as seen by RIS peers, as explained later in this subsection.

The results show that convergence level of the majority of the Root Servers is relatively high, between 50% to 80%, with the exception J- and M-Root that are below 40%. Most Root Servers' convergence are varying over the time, which implies that network changes took place during the period. In general, they have tendency to increase over the time. Some experience sharp increase at one point in time (A, D), some are steadily increasing (K, L), and some are relatively stagnated (I, C). Only D and M-Root that experience a notable temporary decreasing moment.



(a) A-Root

(b) D-Root

(c) F-Root

(d) M-Root

Figure 4.1.: Convergence level of A, F, D, and M-Root. Results for others are available in Appendix A

From the convergence graphs, a number of notable events can be noticed. Obviously, not all events can be explained since it requires the knowledge of complete routing policies implemented at the routers, which is not available in our datasets. Nevertheless, using the BGP routing data obtained from RIPEStat, some events can be explored as the following.

Dramatic Increase of A- and D-Root

The common feature from A- (Figure 4.1a) and D-Root (Figure 4.1b) is that they experience dramatic increase at some point in time.

A-Root is identified to have significant increase in February 2014. To analyze this, we compare data on January 1st 2014 and February 1st 2014. There are 60 and 64 dual-stacked VPs respectively, without any VP from January was absent in the subsequent month. Initially there was only one converging VP, then the number increased to 18 in February. 14 out of those 18 VPs converged due to the change in origin AS for IPv6 prefix (from AS 36623 to AS 36625). Recall from Section 2.3 that A-Root originate their prefixes from multiple ASes, possibly one AS per instance[1]. One major factor contributing in low convergence level of A-Root is due to the difference of IPv4/IPv6 origin ASes as seen by VPs. For example, prior to January 2014, many VPs saw different origin ASes for IPv4 (AS 36625) and IPv6 (AS 36623). Later, IPv6-prefix announced by AS 36623 was withdrawn and originated by AS 36625, which resulted in convergence for VPs that already saw AS 36625 as the IPv4 origin AS.

The sudden increase in D-Root is identified taking place at November 2013. Unlike A-Root, D-Root prefixes are originated from a single AS (AS 27) and the sudden increase is influenced by the changes in its upstream providers configuration. Initially, for IPv4 connectivity, D-Root is identified to have three upstream providers (AS 33657, AS 22925, and AS 10886) with AS 22925 as the main one. Then, around October 2013 D-Root was peered with another upstream provider (AS 42, Packet Clearing House), which immediately replaced AS 22925 to become the dominant upstream. As for IPv6, initially the most connections toward D-Root came through AS 10886. Then, AS 42 replaced its dominance as well. As the result, many diverging VPs that used to reach D-Root via different penultimate AS for IPv4 and IPv6 were switching to use AS 42 for both connectivities

By comparing BGP routing data on October 1st and November 1st 2013, there were 61 and 66 VPs respectively, without any VP in October became absent in November. There were only 4 converging VPs in October, and significantly increased to 32 in the subsequent month. From those VPs in October that have diverging paths, 26 became convergent in November. All of them are because they used AS 42 as the penultimate AS of D-Root. Interestingly, all of them also experienced shorter paths than before. In fact, there were more VPs that switched to AS 42 for their IPv6 paths than their IPv4. To summarize, the decision to use AS 42 as the upstream provider for IPv4 and IPv6 significantly increases the convergence level and shorten the AS path length as well.

Convergence Level Drops Experienced By F- and M-Root

F- (Figure 4.1c) and M-Root (Figure 4.1d) experienced drops in their convergence level for some period of time. Since the number of VPs observing the prefixes fluctuate from time to time, it is rather difficult to observe a trend taking place in a period of time as opposed to, for example, sudden increase in A- and D-Root. Therefore, in this case study we select certain points of the trend and perform comparison on it.

In F-Root case, we categorize it into two periods of drop: *(i)* from July 2014 to December 2014, and *(ii)* from December 2014 to November 2015. To make a comparable

[1] unfortunately, we cannot find official information available for confirmation

analysis, we seek VPs that present at the beginning and the end of each period. Afterwards, we only take VPs that changed its state from converging to diverging by the end of the period.

VP	July 1st 2014	December July 1st 2014
56730	[56730, 6939, 1280, 3557]	[56730, 51945, 39326, 33073, 3557]
	[56730, 6939, 1280, 3557]	[56730, 6939, 1280, 3557]
8607	[8607, 6939, 1280, 3557]	[8607, 3257, 30132, 3557]
	[8607, 6939, 1280, 3557]	[8607, 6939, 1280, 3557]
8758	[8758, 6939, 1280, 3557]	[8758, 15576, 3257, 30132, 3557]
	[8758, 6939, 1280, 3557]	[8758, 6939, 1280, 3557]
29636	[29636, 6939, 1280, 3557]	[29636, 39326, 33073, 3557]
	[29636, 6939, 1280, 3557]	[29636, 6939, 1280, 3557]
49605	[49605, 6939, 1280, 3557]	[49605, 5580, 30132, 3557]
	[49605, 6939, 1280, 3557]	[49605, 6939, 1280, 3557]
57821	[57821, 6939, 1280, 3557]	[57821, 48039, 3257, 30132, 3557]
	[57821, 6939, 1280, 3557]	[57821, 6939, 1280, 3557]
15605	[15605, 6939, 1280, 3557]	[15605, 27320, 3557]
	[15605, 6939, 1280, 3557]	[15605, 6939, 1280, 3557]
8447	[8447, 6939, 1280, 3557]	[8447, 30132, 3557]
	[8447, 6939, 1280, 3557]	[8447, 6939, 1280, 3557]
VP	**December 1st 2014**	**November 1st 2015**
22548	[22548, 30122, 3557]	[22548, 30122, 3557]
	[22548, 30122, 3557]	[22548, 16735, 27781, 28054, 3557]
52888	[52888, 30122, 3557]	[52888, 30122, 3557]
	[52888, 30122, 3557]	[52888, 1916, 6939, 27781, 28054, 3557]
16735	[16735, 22548, 30122, 3557]	[16735, 22548, 30122, 3557]
	[16735, 22548, 30122, 3557]	[16735, 27781, 28054, 3557]
14840	[14840, 30122, 3557]	[14840, 30122, 3557]
	[14840, 30122, 3557]	[14840, 18881, 3549, 6939, 27781, 28054, 3557]
1916	[1916, 30122, 3557]	[1916, 30122, 3557]
	[1916, 30122, 3557]	[1916, 6939, 27781, 28054, 3557]

For each VP, the upper and lower rows represents IPv4 and IPv6 AS paths, respectively

Table 4.1.: Diverging VPs of F-Root during two periods of level drop

Table 4.1 presents the selected VPs for each period. It can be seen that in the beginning of the first period (July 1st 2014), all diverging VPs reached F-Root through upstream AS 1280 for both IPv4 and IPv6. Diverging VPs in the end of the first period (December 1st 2014) are due to the change of IPv4 penultimate AS, *i.e.*, from 1280 to any other. The second period is similar to the first one, except that now it is caused by F-Root instance identified by AS 30122 instead of AS 1280. In contrast to the first period, now the divergence happens due to the change of penultimate AS in IPv6 route (from AS 30122 to 28504).

Recall from Section 2.2 that F-Root uses unique penultimate AS for each of its instance for physical identifier at control-plane level, while originating their prefixes from a single AS. It means that those diverging VPs in Table 4.1 are directed toward different instances for IPv4 and IPv6. Based on PeeringDB data[2], we believe that AS 1280 is the identifier for F-Root global nodes. Therefore, in the first period, the VPs switched from the global nodes to other local instances. By the end of the period, most of them used F-Root local instance in London (identified by AS 33073), while the rest went to the Netherlands (identified by AS 30132). F-Root global nodes are located in United States, and one in Amsterdam. All of these VPs are located in Europe (Milan, Vienna, Amsterdam, and mostly in London). However, their IPv6 route still used the global instance.

Stranger case is identified in the second period. Initially, the VPs in second period (all of them are located in Sao Paulo, Brazil) chose F-Root instance in Sao Paulo (identified by AS 30122) for both IPv4 and IPv6, which is the ideal scenario. However, they later identified to switch using the instance in Sint Marteen, Anguilla (identified by AS 28054), which located in Carribean for IPv6 connection. Both instances are configured as local nodes. The fact that those Sao Paulo VPs saw and selected Carribean instance indicates either Sao Paulo instance's IPv6 service was offline and Sint marteen instance's catchment area was intentionally configured to cover Sao Paulo, or simply route leakage happened during that interval.

Now let us discuss M-Root. M-Root has decreasing and later increasing periods of convergence level (Figure 4.1d). Using similar method used to analyze F-Root, we obtain result in Table 4.2. For the decreasing period, it seems to be caused by different transit AS used to reach M-Root. Two VPs were switched from AS 2200 to AS 2500 for IPv4, which also results in much longer AS path. For the rest, the change is in IPv6 transit AS, where the converging VPs switched to access M-Root via AS 6939 later. For the converging period, the increase of convergence level is partly caused by network expansion of M-Root. It can be seen that previously M-Root have different routing policy for IPv4 and IPv6, with AS 6939 is mainly used as the IPv6 upstream. Later, M-Root decided to make direct peering sessions with many other ASes for both IPv4 and IPv6, resulting in shorter (and converging) AS path.

Why Do M- and J-Root Have The Worst Convergence Level?

Compared to the others, J- and M-Root have the worst convergence level. For J-Root, it is easily understood. J-Root is similar to A-Root in the sense that they also use multiple ASes to announce their prefixes[3]. Thus, diverging paths due to different origin

[2] `https://www.peeringdb.com/asn/1280`

[3] As opposed to A-Root that can be inferred that each AS represents an instance, J-Root seems to group together multiple instances into different origin ASes. Unfortunately, we cannot find official

VP	**Feb 1st 2012**	**Apr 1st 2014**
680	[680, 20965, 2200, 7500]	[680, 20965, 11537, 22388, 7660, 2500, 7500]
	[680, 20965, 2200, 7500]	[680, 20965, 2200, 7500]
9002	[9002, 2497, 7500]	[9002, 2497, 7500]
	[9002, 2497, 7500]	[9002, 6939, 7500]
12859	[12859, 3257, 7500]	[12859, 3257, 7500]
	[12859, 3257, 7500]	[12859, 6939, 7500]
1853	[1853, 20965, 2200, 7500]	[1853, 3356, 2516, 7500]
	[1853, 20965, 2200, 7500]	[1853, 6939, 7500]
1103	[1103, 20965, 2200, 7500]	[1103, 2603, 11537, 22388, 7660, 2500, 7500]
	[1103, 20965, 2200, 7500]	[1103, 20965, 2200, 7500]
29140	[29140, 3257, 7500]	[29140, 3257, 7500]
	[29140, 3257, 7500]	[29140, 6939, 7500]
VP	**April 1st 2014**	**June 1st 2016**
48166	[48166, 12389, 2516, 7500]	[48166, 7500]
	[48166, 6939, 7500]	[48166, 7500]
31019	[31019, 41887, 5580, 2497, 7500]	[31019, 7500]
	[31019, 6939, 7500]	[31019, 7500]
12859	[12859, 3257, 7500]	[12859, 7500]
	[12859, 6939, 7500]	[12859, 7500]
15435	[15435, 3257, 7500]	[15435, 7500]
	[15435, 6939, 7500]	[15435, 7500]
29140	[29140, 3257, 7500]	[29140, 3257, 7500]
	[29140, 6939, 7500]	[29140, 3257, 7500]
12779	[12779, 174, 3257, 7500]	[12779, 7500]
	[12779, 6939, 7500]	[12779, 7500]
34288	[34288, 3257, 7500]	[34288, 7500]
	[34288, 6939, 7500]	[34288, 7500]

For each date, the upper and lower row represents IPv4 and IPv6 AS path, respectively

Table 4.2.: Decreasing (February 2012–April 2014) and increasing (April 2014–June 2016) period of convergence level experienced by M-Root

ASes experienced by a VP can be easily detected, unlike anycast service that uses a single origin AS. However, A-Root have better convergence level than J-Root. We believe that it is because A-Root only has five instances where all of them are global nodes and dual-stacked, compared to 112 J-Root instances with only 12 of them are dual-stacked. Thus, VPs located outside of the catchments of those 12 dual-stacked instances are likely to have diverging paths. Of all diverging VPs throughout the observation period, 57.8% is caused by different IPv4/IPv6 origin ASes. However, it is not just merely about the number of dual-stacked instances. Take J-Root as an ex-

information regarding their anycast configuration.

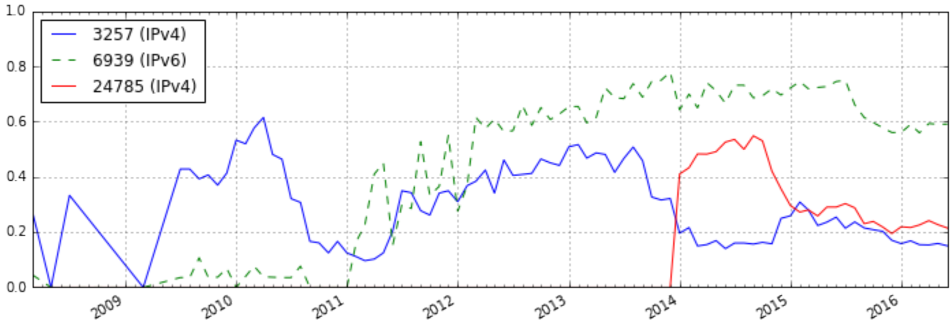


Figure 4.2.: M-Root's most dominant upstream providers

ample. From all of its dual-stacked instances, half of them are located in the same cities as some of RIS collectors. However, it does not automatically translate to better reachability from VP's point of view.

In contrast to J-Root, M-Root only has five instances where all of them are global nodes and dual-stacked. Low convergence level of M-Root is caused by different routing policies for IPv4 and IPv6 that prefer certain providers to transit. Figure 4.2 illustrates M-Root's top upstream providers as seen by RIS collectors. Since 2011, AS 6939 (Hurricane Electric) has been dominating M-Root's IPv6 upstream (more than 50%). On the other hand, the IPv4 connectivities are more distributed among several transit providers/peers. The top IPv4 upstream providers are AS 3257 and AS 24785, which are not as dominant as AS 6939 in IPv6. Thus, low convergence level in M-Root case is due to different upstream providers used to reach M-Root.

Visibility of Root Servers

As explained in the beginning of this section, Appendix A can also be used to understand the visibility of Root Servers as seen by VPs. High number of dual-stacked VPs means high level of visibility, or in another word, larger catchment area. The number of VPs are increasing over the time, which is in line with the expansion of the deployed collectors. This is especially noticeable by the end of 2015, where the figure is significantly increased due to the addition of new collectors (Table 3.2). Ideally, all Root Servers should have relatively similar red line height for a given time, meaning that a similar number of VPs have exposure to those Root Servers. This is not what happens in practice, of course, due to different policies implemented by the operators (amount of deployed instances and its placement, peering agreements, and so on).

Large number of instances supposedly should directly correlate to high visibility, while the amount of dual-stacked instances does not have contribution here since the VPs may take any path towards the instances as long as the instances are configured as global nodes. However, this does not always apply. Root Servers with small number of instances (<10)–A, C, and M-Root–have relatively high level of visibility. The lowest ones are F and I-Root, even though both of them have ~50 instances. More interestingly, all I-Root instances are configured as global nodes, which should have provided higher exposure to the global Internet.

We believe that the reason is because F- and I-Root are lacking of peering connection with large providers that are willing to provide global visibility. A- and C-Root are operated by commercial organizations (Verisign and Cogent, respectively) that run large-scale network infrastructures globally. It allows them to provide better connectivities with the rest of the Internet. M-Root peers with a number of of ISPs, with some of them provide free transit service[4]. On the other hand, F- and I-Root use open peering policy that requires participation from the interested organizations. Free peering sessions are typically used to exchange traffic between each others'networks, but not to reach the rest of the Internet. Thus, it limits the visibility of the Root Servers beyond its peers. However, K-Root also implements the same policy but with larger visibility level. We believe that this is due to the status of RIPE as the operator of K-Root, which have large base of membership in its region. Hence, it is easier for RIPE to promote direct peering between K-Root instances and RIPE members.

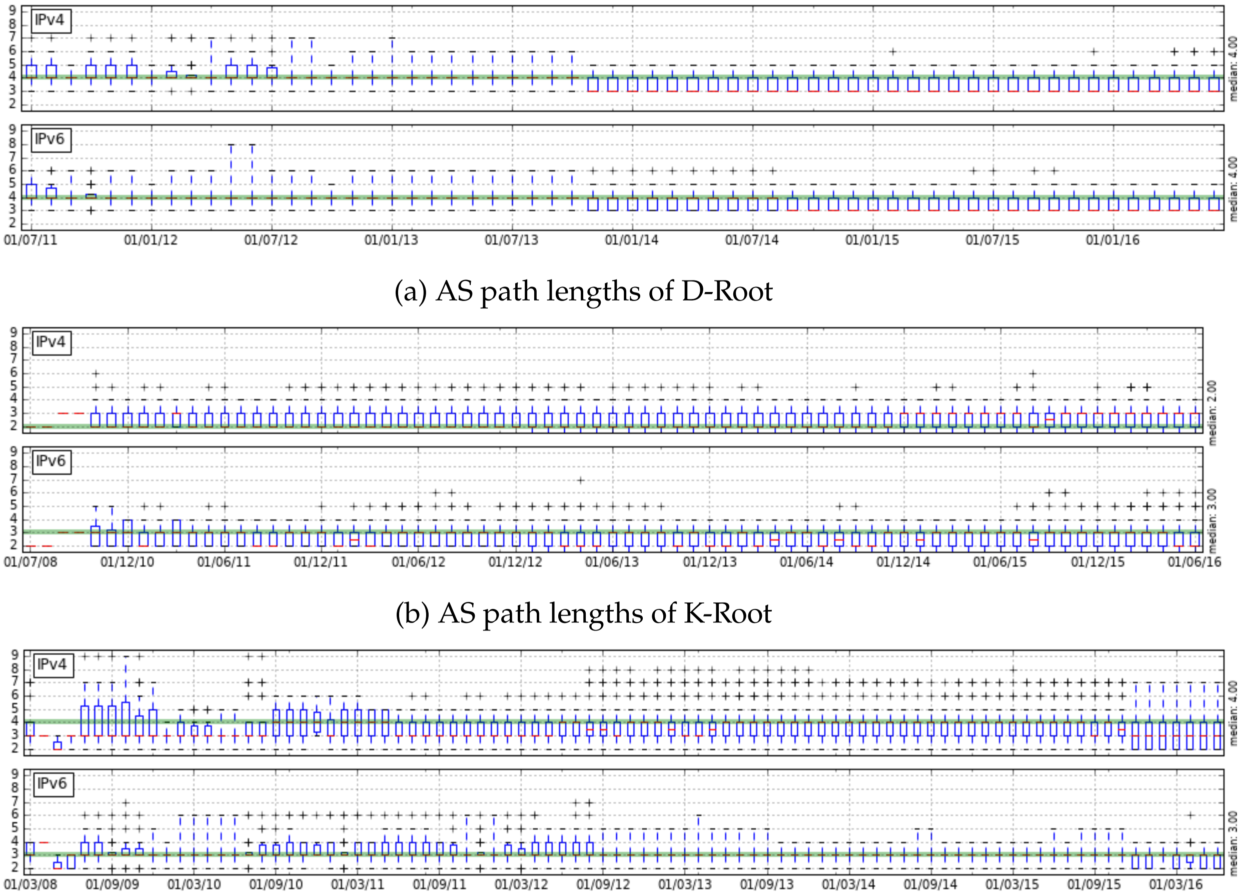
4.1.2. The Trends of AS Path Lengths

Appendix C.1 provides the statistics of AS path lengths of VPs toward all selected Root Servers over the observation period. The green line on all graphs illustrates the median of path length, which is summarized in Table 4.3. Except for A and D-Root, Root Servers do not experience much changes on their path lengths over the time.

Past study shows that the average AS path length tends to get shorter, especially for IPv6 [39]. This is further confirmed by Dhamdhere et al. [27], who concluded that the overall AS path length for IPv6 shows a decreasing trend, and showed sharp decreasing since 2008. As for IPv4, the average AS path length is stable around 4 AS hops. Result from this thesis indicates roughly similar figure. In general, the average IPv4 and IPv6 path length is marginally less than 4, with the difference between them is not significant. Compared to the rest, K-Root has the shortest path length for both IPv4 and IPv6. It generally shows that K-Root has better reachability as seen by VPs. On the other hand, I-Root have the longest average path length, albeit not that significantly different with the rest.

Overall, the difference between IPv4 and IPv6 path lengths for each Root Server is not that much. However, convergence level seems to have effect on it. Root Servers with poor convergence level (M- and J-Root) have the highest differences. J-Root have noteworthy lower IPv4 path length compared to its IPv6. On the contrary, M-Root

[4] http://m.root-servers.org/



(a) AS path lengths of D-Root

(b) AS path lengths of K-Root

(c) AS path lengths of M-Root

These are the box plots which represent the distribution of AS path lengths of the respective Root Servers. The central rectangle comprises of three parallel horizontal lines representing the first quartile, the median (red), and the third quartile. The whisker below the rectangle represents the minimum value, while the top whisker is the maximum one. The outlier data is depicted as crosses. The green line represents the average of the median over the time

Figure 4.3.: AS path lengths of D, K, and M-Root

have prominently lower IPv6 path length than its IPv4. It shows that J and M-Root have stronger connectivity on either protocol.

Appendix C.1 can be used to see the stability of the AS path length over the time as well. C, K, and L-Root are relatively stable. It means that there was not major network configuration changes affecting the path length from the VPs. D-Root (Figure 4.3a) looks to have two phases of its path length dynamics. The fluctuated path length of D-Root VPs started to stabilize at November 2013, the same time when D-Root started to use AS 42 as one of their upstream (Section 4.1.1). This decision seemed to help D-Root gaining lower average path lengths than before, and since then the path length did not vary much. M-Root IPv6 path length (Figure 4.3c) looks similar to D-Root. Starting from September 2012, the path lengths started to stabilize. IPv6 path lengths of M-Root's VPs are mostly 3 (indicated by flat rectangle at 3), which shows that they

Root Server	Median		Mean	
	IPv4	IPv6	IPv4	IPv6
A	4	3	3.79	3.64
C	4	4	3.68	3.77
D	4	4	3.78	3.75
F	4	4	3.65	3.67
I	4	4	3.86	3.90
J	3	3	3.18	3.62
K	2	3	2.56	2.65
L	3	3	2.95	3.03
M	4	3	3.68	3.10

Table 4.3.: Median and mean of IPv4 and IPv6 path lengths over the time

use an upstream provider that have large connectivities, which is AS 6939 (Figure 4.2). For A-Root, the path lengths were highly varying until the beginning of 2014, when the length started to stabilize. We believe that the discussion of A-Root in Section 4.1.1 also takes part in this dynamics.

The graphs in Appendix C.1 also inform us about the symmetry of the catchment topology. Ideally, an anycast catchment topology should be in the form of tree(s) where the origin AS of anycast service serves as the center of tree (or their upstream provider(s)), and all end-user ASes should have relatively similar path lengths. It demonstrates that the anycast instances provide good reachability from any corner of the Internet, and that the instances are properly distributed. Quantitatively, this behavior is indicated by a box plot with narrow range of upper and lower whiskers, and as few outliers as possible. C-Root (Figure C.2) is a good example of it. The extreme contrasting example is M-Root's IPv4 path length. M-Root's poor IPv4 statistics compared to its IPv6 is not because of the overall poor connectivities, but largely contributed by small number of VPs that have quite long paths (marked as outliers in Figure C.9). It may serve a good indicator on planning new peering agreement or even new instance deployment to provide better connectivities.

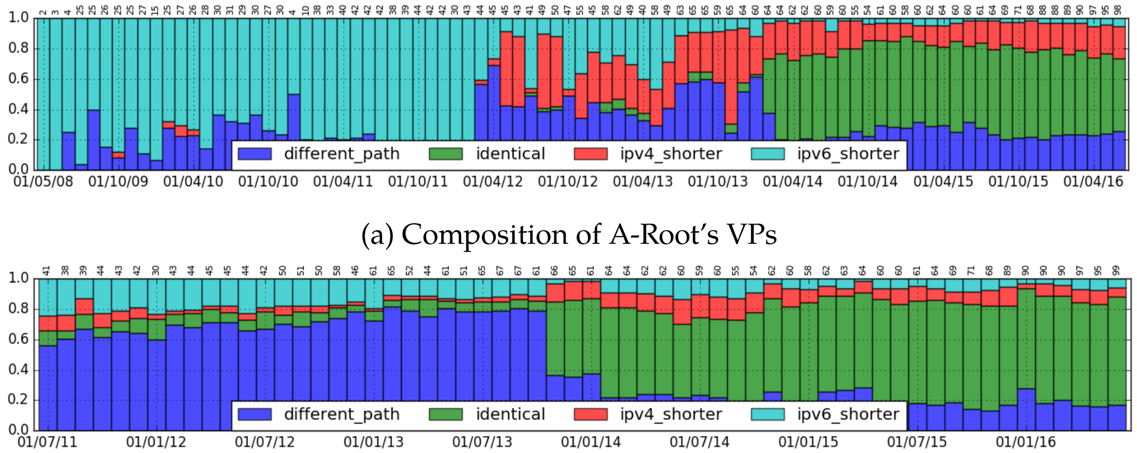
4.2. The Differences Between IPv4 and IPv6 Catchment Areas

Previous section discusses about the dynamics of anycast catchment areas over the time in terms of the convergence level and the trends of AS path length. It uses data from all VPs as long as they have both IPv4 and IPv6 routing information toward Root Server. In this section, we focus our discussion on the differences between IPv4 and IPv6 catchment areas itself. Therefore, we focus only on diverging VPs of certain Root Server at a given time. The definition of different AS paths used in this thesis is provided in Section 3.3. With current data we have in our disposal, we can not answer the question of *why* exactly the differences take place, since it requires the knowledge of BGP routing configuration on each routers. However, we can find out *to what extent* the differences affecting the catchment areas, as seen from control-plane perspective.

We start off by discussing the composition of VPs (Section 4.2.1). Next, the average path length (Section 4.2.2), followed by how different is it path-length-wise (Section 4.2.3).

4.2.1. Composition of VPs

Different paths encountered by a diverging VP may still result in similar path lengths, or it could also result in either IPv4 or IPv6 shorter path. Section 4.1.1 specifically focuses on the fraction of converging VPs of all dual-stacked VPs. Here, we are interested to look deeper at the diverging VPs: how many diverging VPs that experience shorter IPv4 path, shorter IPv6 path, or similar path lengths. By breaking down the composition of all VPs based on its IPv4/IPv6 path lengths, we present the results in Appendix B with Figure 4.4 showing composition of A and D-Root's VPs serves as an example. Root Servers have more diverging VPs with equal IPv4/IPv6 path lengths than shorter IPv4/IPv6 path, except for J, I, and M-Root. I-Root itself has slightly more diverging VPs with shorter IPv6 paths. Root Servers with low convergence level (J and M-Root) have noticable shorter paths. J-Root is dominated by VPs with shorter IPv4 path. On the contrary, VPs with shorter IPv6 path dominate M-Root.



(a) Composition of A-Root's VPs

(b) Composition of D-Root's VPs

The bins represent the fraction of VPs for each category. The number on top of the bin shows the total number of VPs at a time

Figure 4.4.: Composition of A and D-Root's VPs

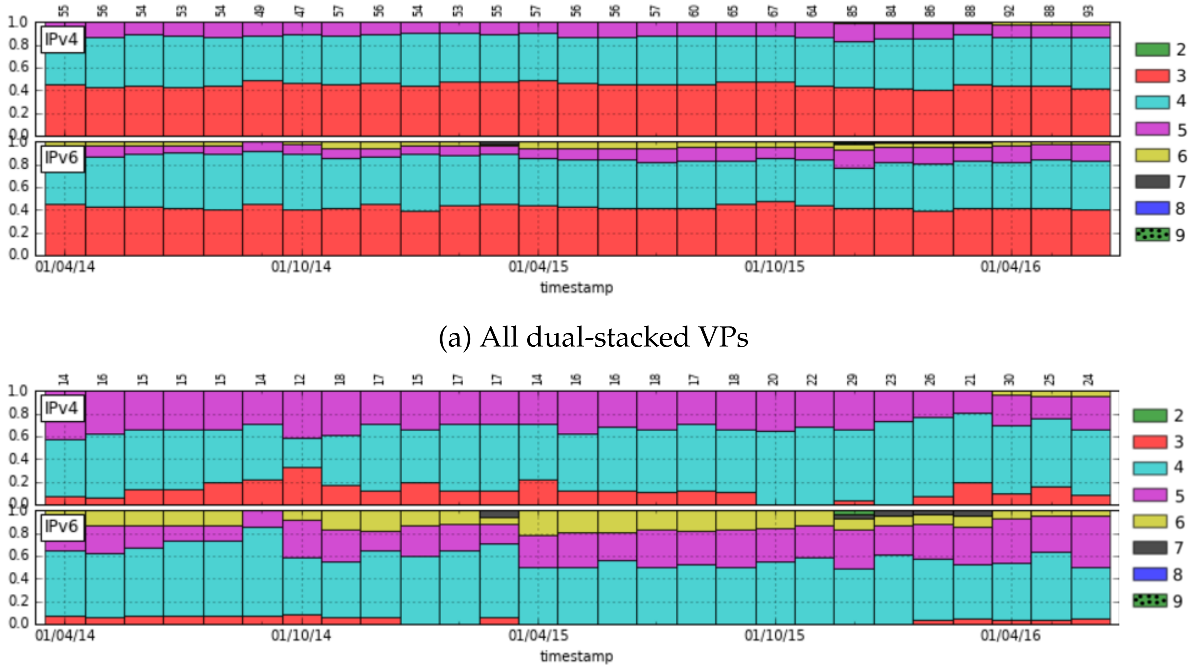
Diverging paths with equal lengths is largely due to coincidence. However, there are some special cases, for example in D-Root (Figure 4.4b). It has large fraction of VPs with diverging path and equal length prior to November 2013. We have discussed in Section 4.1.1 that prior to November 2013, the dominant upstream was AS 22945. AS 22945 itself is identified to have all connectivities by transiting via AS 6939. The similar case also happens in IPv6, now with AS 10886 as the upstream. In D-Root case, VPs with diverging paths and equal length prior to November 2013 mostly happened because the VPs reached D-Root through AS 22945 for IPv4 and through AS 10886 for IPv6, with AS 6939 as the intermediate transit AS. VPs path via AS 6939 were always the same (regardless IPv4/IPv6), the only difference is the penultimate AS before reaching D-Root's origin AS. After the introduction of AS 42, the catchment topology changed, since most VPs switched to reach D-Root via AS 42.

Prior to February 2012, A-Root (Figure 4.4a) was dominated by VPs with shorter IPv6 paths. It is because A-Root directly peered with AS 6939 and all IPv6 connectivities were through them. This is also one of the reasons why A-Root had such low convergence level during that period, as AS 6939 is the dominant IPv6 transit provider thus A-Root's VPs experienced shorter IPv6. Starting in March 2012, they started to use other IPv6 transit providers as well, resulting in the VPs no longer got shorter IPv6. We believe that this event lead to higher A-Root IPv6 path lengths starting from march 2012 in Figure C.1.

4.2.2. Average Path Length

We have discussed the trends of AS path lengths for all VPs in Section 4.1.2. Here, we focus only on average path length of diverging VPs. The complete result is presented in Appendix C.2, and summarized in Table 4.4. To get the knowledge of the quantity of VPs for each AS path lengths, we break down the data to get the VPs degree (relative to the Root Server) in Appendix D.

Intuitively, the longer the path the higher the probability of having diverging paths is. In general, the results in Appendix C.2 exhibit similar patterns with the ones in Appendix C.1. This is because of two factors: *(i)* the number of diverging VPs are not significant to influence the overall path length distribution, *(ii)* diverging VPs are generally have longer paths, but not that much, as we see later. Comparing results in Table 4.4 and Table 4.3, we see that Root Servers with high convergence level, especially C-, I-, and K-Root, have the largest differences. This is especially noticeable for C-Root, the one with the highest differences (0.53 hop for IPv4 and 0.76 hop for IPv6) by comparing Figure C.2 and Figure C.11. The contrast of C-Root's average path lengths between all dual-stacked VPs and diverging VPs only are depicted in Figure 4.5. Root Servers with low convergence level, J- and M-Root, only slightly differ because the diverging VPs dominate the statistics in Table 4.3. It means that the diverging VPs mostly have longer AS path lengths than the average, thus confirming the hypothesis.



(a) All dual-stacked VPs

(b) Diverging VPs only

The bins represent the fraction of VPs for each category. The number on top of the bin shows the total number of VPs at a time

Figure 4.5.: C-Root's VP degree

Root Server	Median		Mean	
	IPv4	IPv6	IPv4	IPv6
A	4	4	4.03	3.82
C	4	4	4.21	4.53
D	4	4	4.09	4.04
F	4	4	3.83	3.88
I	4	4	4.29	4.37
J	3	4	3.20	3.70
K	3	3	2.86	3.13
L	3	3	3.09	3.24
M	4	3	4.00	3.22

Table 4.4.: AS path lengths for diverging VPs

4.2.3. How Different Is It?

For VPs with either shorter IPv4 or IPv6 paths, it is interesting to find out to what extent the path length difference is. The average differences for shorter IPv4 and IPv6

Root Server	Shorter IPv4	Shorter IPv6
A	1.07	1.23
C	1.49	1.21
D	1.12	1.09
F	1.32	1.21
I	1.32	1.41
J	1.41	1.16
K	1.1	1.17
L	1.24	1.66
M	1.03	1.43

Table 4.5.: Average AS path length differences

paths are calculated for each Root Server and presented in Appendix E and Appendix F, respectively.

Table 4.5 summaries the results in Appendix E and Appendix F. In general, the average AS path difference for both shorter IPv4 and IPv6 is ~1 hop. For shorter IPv4 path, C- and J-Root have the largest differences. C-Root (Figure E.2) has consistent number of VPs with 1 and 2 hops of path differences, while J-Root (Figure E.6) used to have varying AS path differences (up to 3 hops) until February 2014. Interestingly, this coincides with the notable increase of its convergence level (Figure A.1f). For shorter IPv6 path, L- and M-Root have the largest differences. Varying path differences (>1 hop) in L-Root (Figure F.8) take place sporadically. However, once it happens, it consists of large differences (3 to 4 hops). For M-Root, the varying path differences started to happen regularly from July 2012.

There is trend among large content providers to conduct direct peerings with networks hosting large number of end-user prefixes, in order to bring their services closer to their clients [16]. This results in one AS hop connection between user and the provider. The similar approach is also indicated to be used by some Root Servers, especially those that implement open peering policy.

One major contributing factor of diverging paths is the practice of direct peering on either IPv4 or IPv6, while the other protocol still need to reach Root Server via transit ASes. Take VP in AS 286 for example. It had diverging paths to reach M-Root between September 1st 2009 to February 1st 2012. AS 286 was directly peered to M-Root for IPv4 connectivity, while for IPv6 it transited via AS 3257.

Table 4.6 presents the fraction of direct peering from VPs with shorter IPv4/IPv6 paths. It should be noted that C- and I-Root origin ASes are run behind their own operators' ASes (Cogent and Netnod, respectively) , hence in their case the direct peering is defined by peering connection between VPs and their upstream ASes. D-Root do not have direct peering because it uses two upstream providers (PCH and MAXGigaPOP)

Root Server	Shorter IPv4 (%)	Direct peering (%)	Shorter IPv6 (%)	Direct peering (%)
A	16.86	0.98	27.3	8.47
C	8.44	38.78	2.7	31.91
D	7.4	0	10.46	0
F	13.08	53.65	12.42	33.78
I	22.05	65.14	17.7	15.68
J	42.62	34.1	13.66	16.78
K	13.53	69.42	4.87	78.4
L	12.23	51.44	4.69	27.23
M	5.95	47.48	44.84	4.12

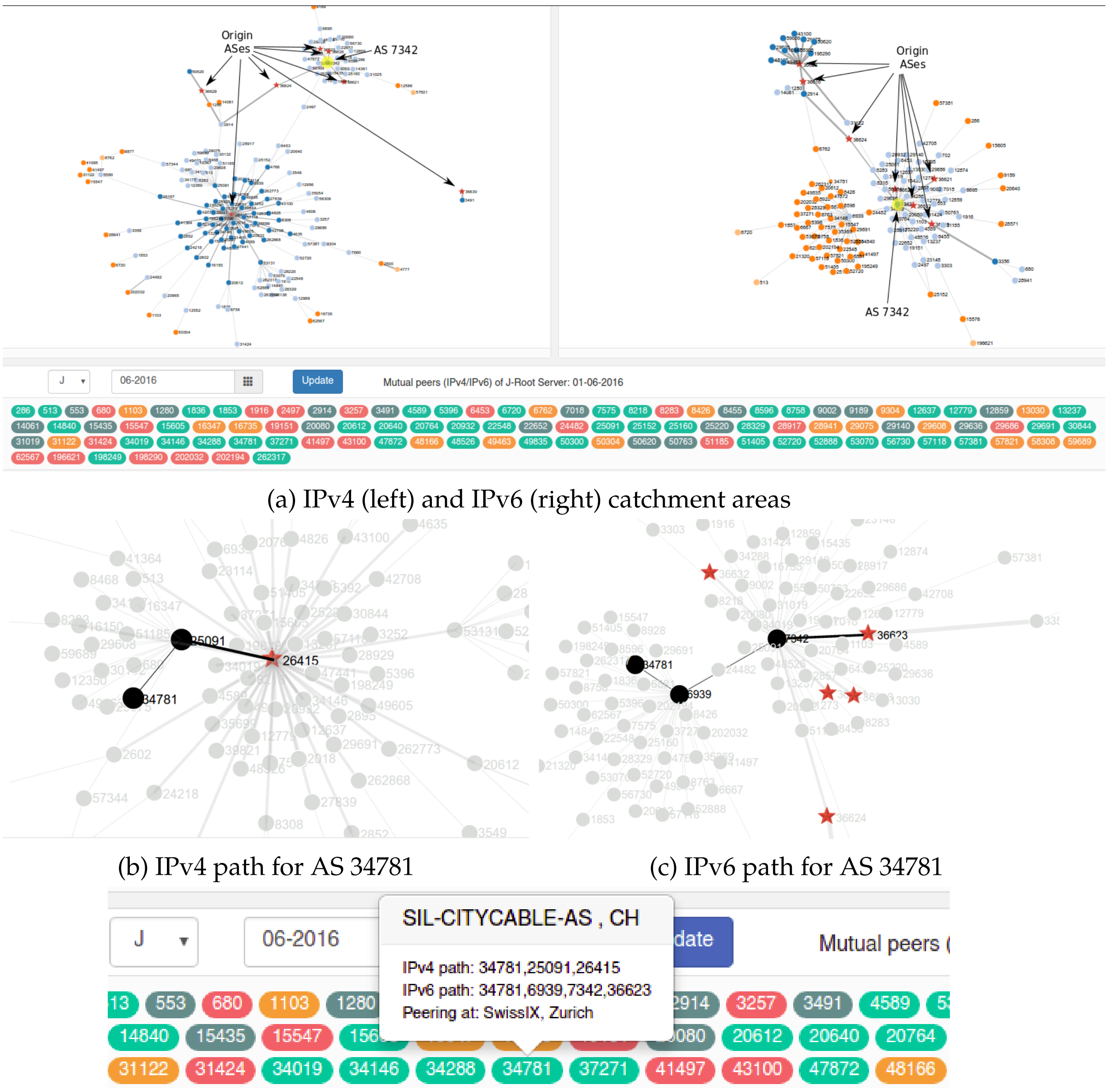
Table 4.6.: Fraction of direct peerings from VPs with shorter IPv4 and IPv6

to reach the Internet. For other Root Servers operated by non-profit organizations (F, I, K, L, M), direct peerings between the Root Server's AS and VPs become the major factor of shorter IPv4 path. For shorter IPv6, only K-Root that dominated by direct peering (78.4 %). This shows that IPv6 direct peering is not as common as in IPv4, possibly due to lack of IPv6-enabled ASes to be peered with.

4.3. Visualizing Anycast Catchment Areas

Figure 4.6 represents the result of our tool visualizing J-Root catchment areas as seen by RIS at June 1st 2016. J-Root is selected because it has the lowest convergence level, thus it provides good example for the visualization. Figure 4.6a represents the J-Root catchment areas for IPv4 (left) and IPv6 (right) on June 1st 2016. The origin ASes of J-Root prefixes are represented by red star icon. AS level relative to origin ASes is represented by colors: in this example dark blue represents level 1, light blue level 2, orange level 3, and so on.

From Figure 4.6a, it can be immediately seen that J-Root has distinct catchment areas. AS 7342 (marked with yellow circle) was one of the upstream providers used by J-Root. In IPv4 catchment, its role is not significant. Only few VPs reached J-Root through it, possibly due to localization policy. In contrast, AS 7342 becomes the dominant upstream provider in IPv6 catchment, where most of VP paths toward J-Root traversed through it. We may also see that in IPv6 catchment, many VPs has AS 6939 (Hurricane Electric) as their transit AS. This is in contrast with IPv4 catchment where there is no dominant provider as the transit. Thus, this visualization will help operator to get an idea which upstream they use is more dominant than the other. Furthermore, it can be also extended to provide visualization whether their local instance configuration is leaking or not.



Mutual peers (IPv4/IPv6) of J-Root Server: 01-06-2016

286 513 553 680 1103 1280 1836 1853 1916 2497 2914 3257 3491 4589 5396 6453 6720 6762 7018 7575 8218 8283 8426 8455 8596 8758 9002 9189 9304 12637 12779 12859 13030 13237 14061 14840 15435 15547 15605 16347 16735 19151 20080 20612 20640 20764 20932 22548 22652 24482 25091 25152 25160 25220 28329 28917 28941 29075 29140 29608 29636 29686 29691 30844 31019 31122 31424 34019 34146 34288 34781 37271 41497 43100 47872 48166 48526 49463 49835 50300 50304 50620 50763 51185 51405 52720 52888 53070 56730 57118 57381 57821 58308 59689 62567 196621 198249 198290 202032 202194 262317

(a) IPv4 (left) and IPv6 (right) catchment areas

(b) IPv4 path for AS 34781

(c) IPv6 path for AS 34781

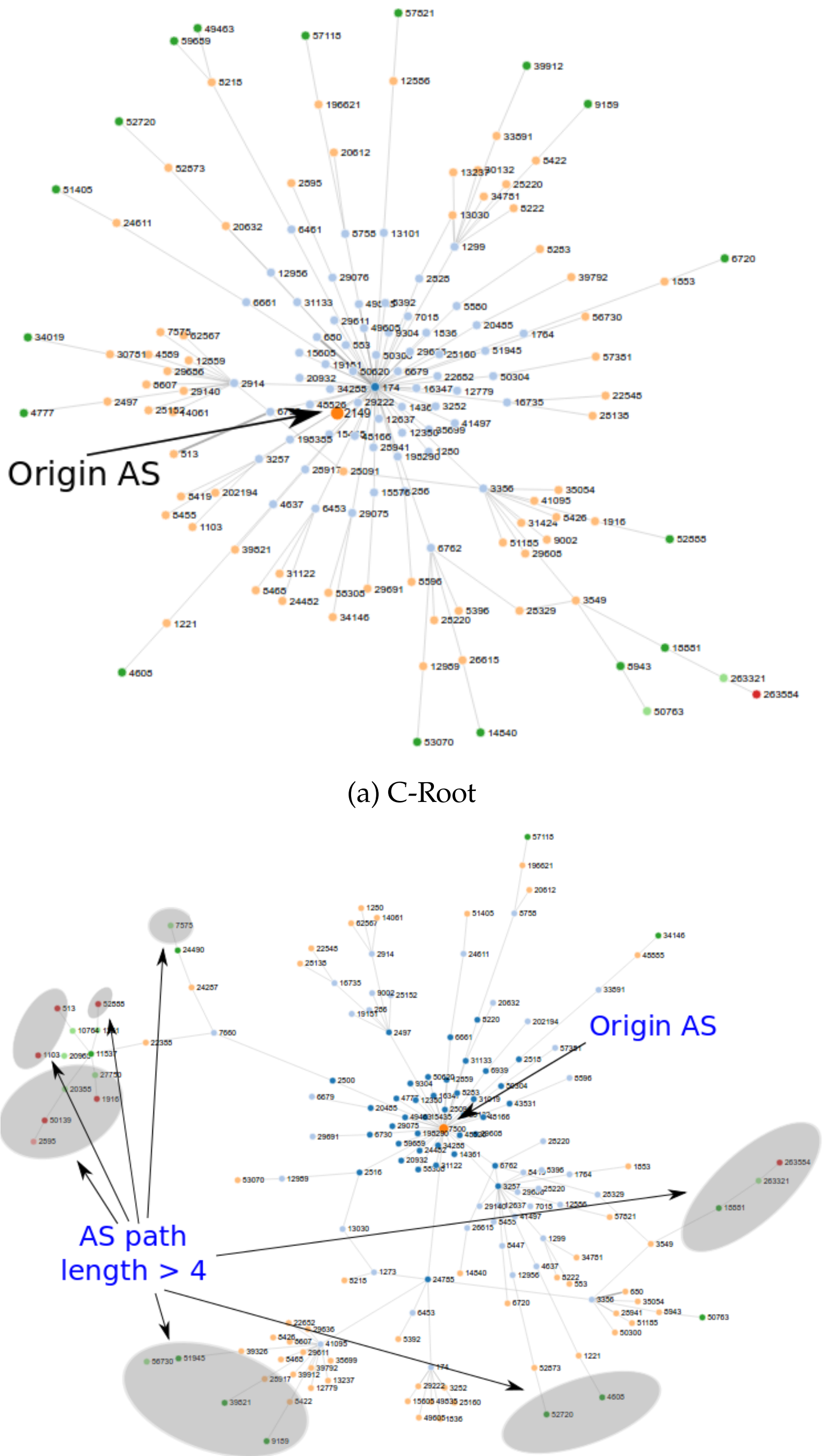
SIL-CITYCABLE-AS , CH

IPv4 path: 34781,25091,26415
IPv6 path: 34781,6939,7342,36623
Peering at: SwissIX, Zurich

(d) Hovering to get information about AS information and IPv4/IPv6 paths

Figure 4.6.: Visualization of J-Root catchment areas at June Ist 2016

On the bottom of Figure 4.6a, mutual VPs in both IPv4 and IPv6 catchments are listed. They have different color scheme to represent whether they have identical paths (grey), shorter IPv4 (blue), shorter IPv6 (orange), or diverging path with equal length (red). Hovering one of these mutual VPs will highlight both IPv4 and IPv6 paths, the AS information retrieved from Cymru via WHOIS service, and at which location the VP peers with RIS collector at. Figure 4.6d shows that AS 34781 is owned by Sil Citycable, a Switzerland-based ISP, and its router is peered with collector at Zurich. The



(a) C-Root

(b) M-Root

Figure 4.7.: C- and M-Root IPv4 catchment areas (January 1st 2016)

hovering action also results in Figure 4.6b and 4.6c. It can be seen that not only it has diverging path, but it also reaches different origin ASes of J-Root (IPv4 uses AS 26415, IPv6 uses AS 36623), which indicates that Sil Citycable customers are served by different J-Root instances for IPv4 and IPv6 queries.

Recall from Section 4.1.2 that an ideal anycast catchment area should be in the form of tree where the origin AS (or its upstream provider's AS) or ASes becomes the center of the tree(s), and the AS path lengths of the end users' ASes should be relatively similar and as short as possible. Poor catchment area would be in the form of a tree where notable number of VPs suffer long AS paths (>4 AS hops[5]) and the topology is unbalanced. The presence of notable number of VPs that possess long AS path indicates that the Root Server should provide better connectivity to them. It could be possibly by expanding the direct peering connections or using transit service from ISP with larger footprint in the Internet. If the VPs are identified to be physically far from its closest instance, then it serves as good indicator to add another new instance.

C-Root is an example of anycasted service of what we believe to have good catchment area (Figure 4.7a), where it has relatively short paths of which enjoyed by all VPs (confirmed in Figure C.2). On the other hand, IPv4 M-Root (Figure 4.7b) is an example of poor catchment, since there are many VPs suffering from long AS path. This is reflected as well in its average IPv4 path length graph (Figure C.9) as discussed in Section 4.2.2.

4.4. Discussion

The previous section showed in details about how different IPv4 and IPv6 catchment areas of each Root Servers. Some questions may arise: what does this mean for operator? Does low convergence level automatically mean bad configuration? Above it all, the fundamental question is: *Why assessing the differences is important*?

As it is already known, IPv6 adoption is still low albeit the accelerating rate [23]. On the other hand, we are now in the phase where IPv6 is already maturing and the major difference between IPv4 and IPv6 is in control-plane [47]. This difference itself is expected to get lower, since the IPv6 network deployments are converging to the existing IPv4 networks [27]. While it is true that both networks are in the process of converging, it should be noted however, during the transition period services running on IPv6 should be ensured that they have comparable–if not better–quality as if it is run on IPv4, so that people are encouraged to migrate. It can only be accomplished by understanding the performance of the service on IPv4 and IPv6, and this study–measurement at control-plane level–is one of the necessary efforts. Revealing

[5] we base this on the result in [39] which stated that the average AS path length is around 4 AS hops

the differences at control-plane level also means that potential performance problems are revealed as well. As [27] shows, different IPv4 and IPv6 AS paths could lead to much worse performance. This is especially important in anycast, since different routing decision may result in the use of different anycast instances.

Thus, having good convergence level is preferable for an anycast service, since it more likely provides comparable service quality in both IPv4 and IPv6. However, there is also cases where different path between IPv4 and IPv6 might be useful. For example, if one of the transit AS have congestion that slows down the connection for IPv4 (which cannot detected by BGP), then the IPv6 connection can be used to provide better connectivity.

5. Conclusions and Future Work

Conclusions drawn from the results of this work is presented Section 5.1. It serves as the answers to research questions of this thesis as well. Finally, suggestions for future works are provided in Section 5.2.

5.1. Conclusions

In Chapter 2, we see that control plane measurement of anycast service can be done by monitoring the address prefixes using BGP routing information provided by BGP speakers. Among other alternatives, the use of BGP data provided by monitoring projects such as RIS or RouteViews is the preferred approach for this thesis. Then, in the beginning of Chapter 3, we make justification to only use data from RIS due to time and resource constraints, since it provides access to the BGP resources using REST API, instead of directly working with the dump files which requires large resources.

In Section 4.1, we show the evolution of Root Servers' IPv4 and IPv6 catchment areas as the following. Most Root Servers have tendency of increasing convergence level over the time. In general, the convergence level of Root Servers is relatively high, between 50% to 80%, with the exception J- and M-Root (below 40%). Some Root Servers experience sharp increase (A and D-Root), and some are relatively stagnated (I, C, and L-Root). Particular exception is for F and M-Root which have temporary moment of decreasing. The changes in convergence level is mostly due to the switch of upstream providers for either IPv4 or IPv6. In terms of Root Servers' visibility as seen by VPs, it is the peering policies which determines it, not the amount of instances deployed. The overall average path length itself is close to 4 hops, which in line with result of similar studies in the past. Furthermore, with the exception of A and D-Root, Root Servers seem not to experience major change on their path lengths over the time.

As for the catchment differences itself, as discussed in Section 4.2, diverging VPs are mostly dominated with VPs with equal path lengths, with J and M-Root (which are the ones with low convergence level) as the notable exception. J-Root is dominated with shorter IPv4, while M-Root is dominated with shorter IPv6 paths. In terms of average path length, the diverging VPs is slightly longer than the ones of dual-stacked VPs. Furthermore, Root Servers with high convergence level (C, I, and K-Root) have the largest differences. For diverging VPs with different path lengths, the average length difference is only 1 hop. Finally, one factor largely contributing diverging paths is the practice of direct peering for either IPv4 or IPv6, while the other protocol is still using transit ASes. The practice of direct peering itself is much more commonly used in IPv4 than in IPv6, except for K-Root that have large fraction of it for both protocols.

Finally, the features of our visualization tool described in Section 4.3 can be used by operator to quickly perform comparison between IPv4 and IPv6 catchment areas. In case of Root Servers with multiple origin ASes or unique penultimate ASes, it can be used as well to detect route leakage and different serving instances for IPv4 and IPv6. It also provide depiction of the symmetry of catchment areas. Good catchment area is indicated by more or less equal AS path length for all VPs. Catchments with unbalanced tree is determined by noticeable number of VPs suffering long AS path, This indicates that the Root Server should provide better service to them.

5.2. Future Work

As discussed in Section 2.4, there are several limitations with the use of public BGP data from measurement projects such as RIS. The biggest concern is that they do not represent the Internet at all with very limited view over the networks, since the collectors are deployed only at few IXPs. Nevertheless, this is the best option available during our work. Immediate improvement to enrich the datasets can be done by using BGP data from RouteViews, as they put collectors at some different locations as RIS. It will provide more complete view of the networks over Root Servers' catchment areas. BMP is the promising alternative, as it allows us to gather all BGP routing data from a BGP speaker (including routes from peers of a peer). However, it requires the router to implement BMP as well, which might require some time to upgrade the routers in IXPs to include such capability. Nevertheless, it seems to be the go-to direction for measurement projects in the future, as already initiated by RouteViews and Caida.

In this thesis, we analyzed BGP data from VPs during the observation time. We take the snapshot of route information for Root Servers' prefixes. In this way, we can draw conclusion about the evolution of the route. However, we only take snapshot once per month. BGP RIB only provides the result of BGP routing calculation, not what triggers the calculation (*i.e.*, the routing events such as prefix withdrawal, announcement, or changes). To study the dynamics of an anycast service from control plane perspective in a finer resolution (*e.g.*,route stability), a further study on BGP update messages of the respective prefixes is necessary. It should be noted, however, that this might requires much more resources since we have to analyze *all* BGP updates during the period, instead of picking up periodic samples.

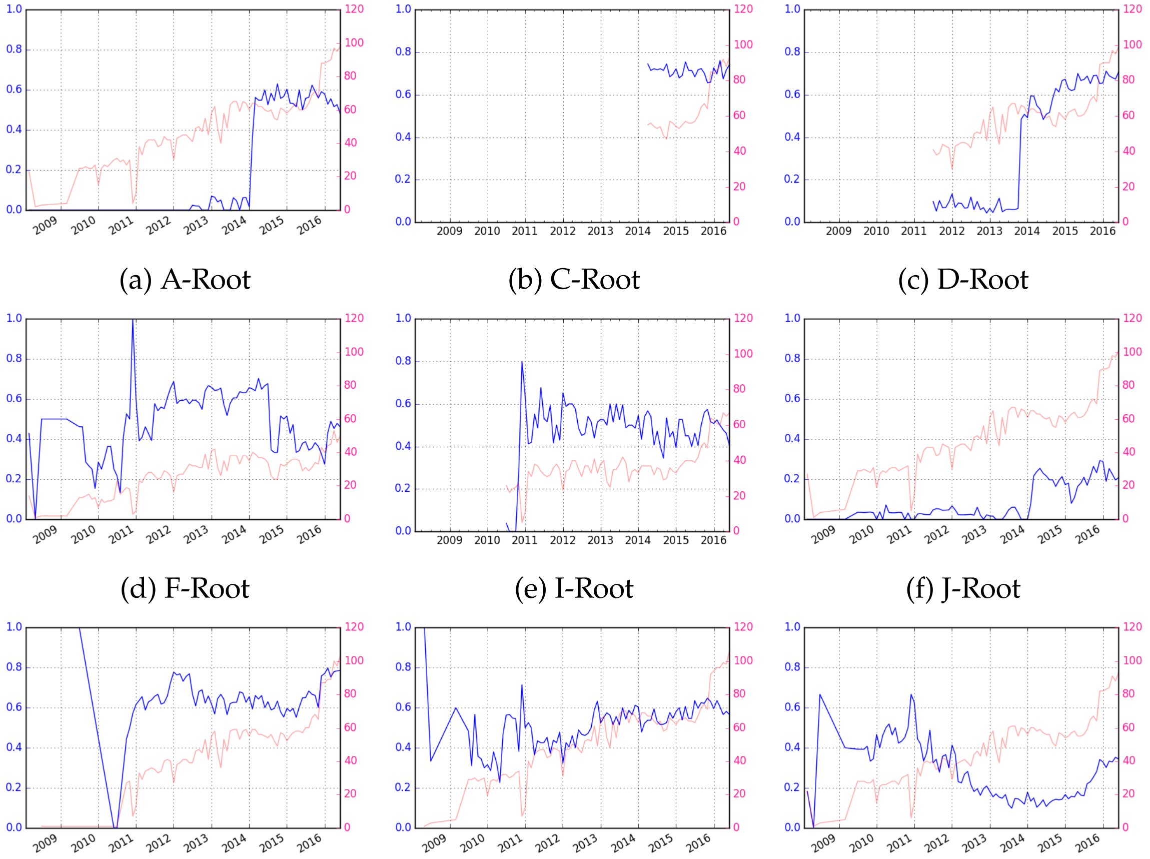
In our analysis, we use the variable AS path length extensively. However, the length of AS path does not automatically correlate to the performance level experienced by end user. For example, in A-Root case, there are situations where VPs have different IPv4/IPv6 origin ASes, while the paths are identical up to the penultimate AS hop (equal lengths). This strongly indicates that end users reside within those VP networks are directed towards different IPv4 and IPv6 instances, which is very likely to be located in different locations. Thus, the performance of both protocols would be different, even though the path length is the same. Another case is for Root Servers with single origin AS that use only few upstream providers for all of its instances. Even if the IPv4 and IPv6 paths of a certain VP is identical, there is a possibility that IPv4 and IPv6 traffic are still routed towards different instances. AS path length also does not provide us information about cold-potato routing[1] in transiting ASes, which could lead to longer delay. The only way to measure the real performance is by conducting data-plane measurement such as `traceroute` or special DNS queries.

In this thesis, the visualization tool is served as proof-of-concept. Currently, it only uses historical data retrieved from RIS. It can be easily extended to dynamically retrieve data directly from RIS to provide near-real-time visualization. It can also be modified to retrieve data from other sources, such as live streaming from RouteViews or from OpenBMP in the future, to provide more comprehensive data. The visualization can also be combined with data-plane measurement and server monitoring to provide complete view of the system. Furthermore, an autonomous monitoring system based on MAPE-K [22] can be developed, so that a change detected in the routing system or server load that exceeds certain threshold may automatically trigger some follow-up action *e.g.*, to boot up new instances in some underserved areas.

[1] the tendency to keeps traffic inside a single AS as long as possible, usually implemented by providers for their customers' traffic

Appendices

A. Convergence



(a) A-Root

(b) C-Root

(c) D-Root

(d) F-Root

(e) I-Root

(f) J-Root

(g) K-Root

(h) L-Root

(i) M-Root

Figure A.1.: Convergence level

B. VPs Composition

A mutual VP can have either diverging or converging IPv4/IPv6 paths. For diverging paths, it can be: *(i)* have shorter IPv4 path, *(ii)* have shorter IPv6 path, or *(iii)* have equal path length. The following graphs represent the VPs composition in terms of the aforementioned categorization for each Root Server. To provide better readability, the height of each stacked bar is normalized and the total number of VPs per time is displayed at the top of the graph.

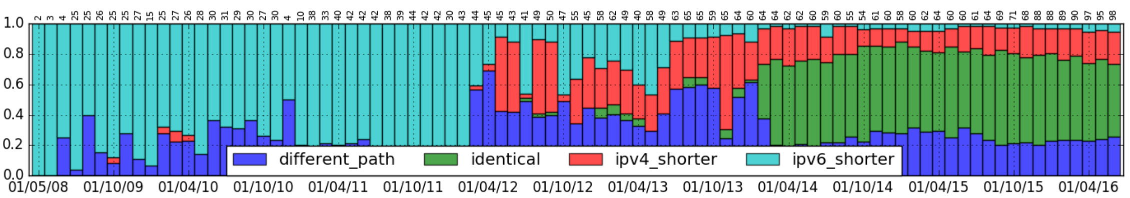


Figure B.1.: A-Root peers composition

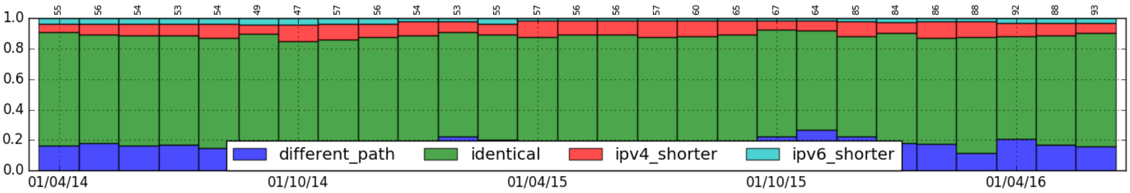


Figure B.2.: C-Root VPs composition

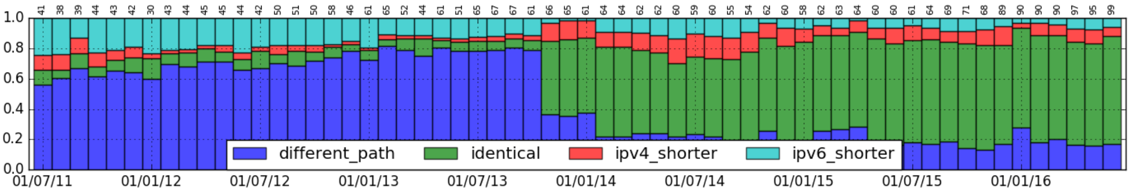


Figure B.3.: D-Root VPs composition

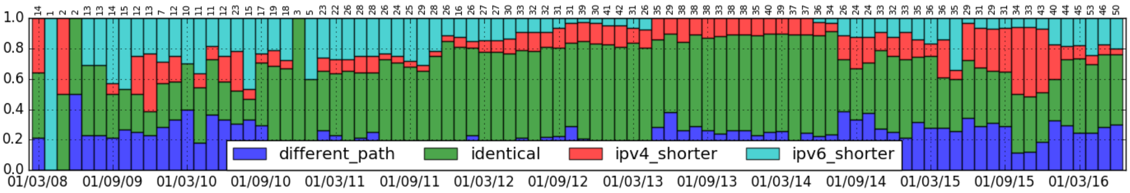


Figure B.4.: F-Root VPs composition

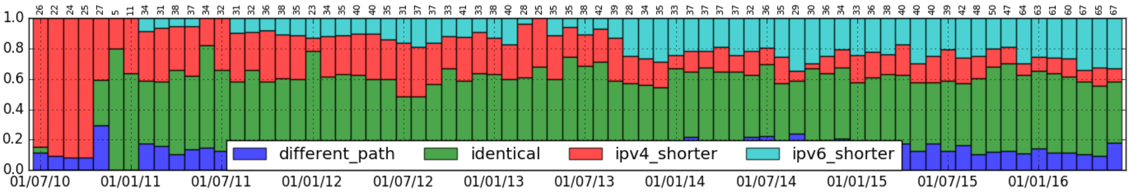


Figure B.5.: I-Root VPs composition

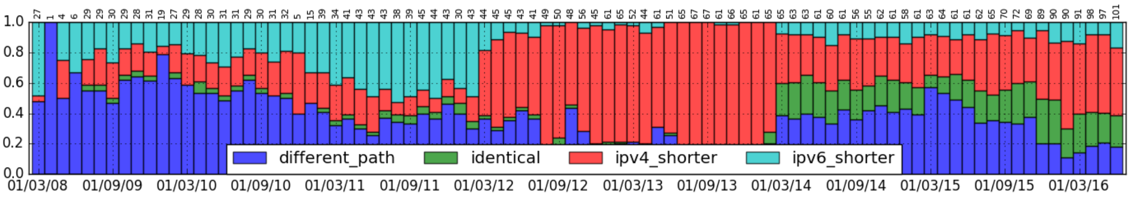


Figure B.6.: J-Root VPs composition

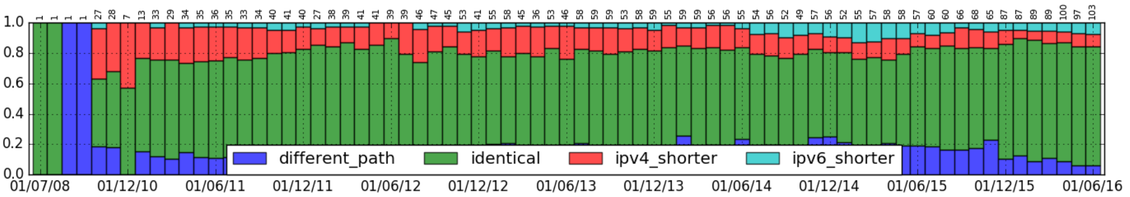


Figure B.7.: K-Root VPs composition

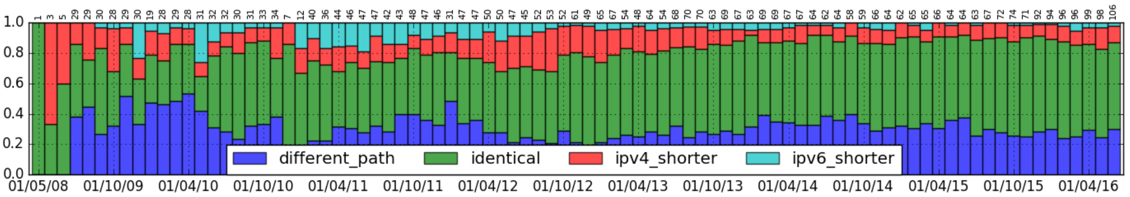


Figure B.8.: L-Root VPs composition

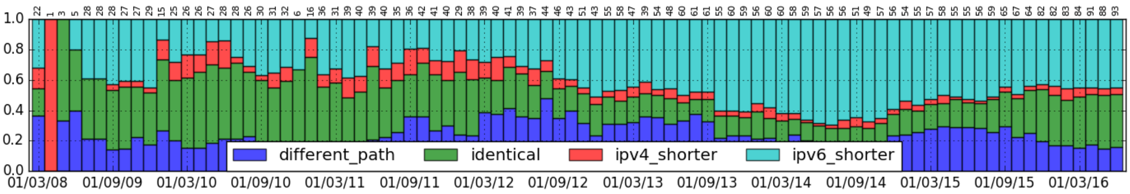


Figure B.9.: M-Root VPs composition

C. AS Path Length Distribution

The box plot is generated using Matplotlib with default configuration. The closed box comprising of three horizontally parallel lines represents the 1st quartile, the median, and the 3rd quartile (bottom to top). Interquartile range (IQR) is defined as the range between 1st quartile and 3rd quartile. The top whisker represents the maximum value below 75% + 1.5 IQR, while the bottom one represents the minimum value above 25% - 1.5 IQR. Any value falls outside those boundaries are regarded as outlier (plotted as '+'). The green line represents the median of all path length values over the time.

Appendix C.1 represents AS path length distribution for all mutual VPs, regardless diverging or converging. Appendix C.2 represents the distribution only for diverging VPs.

C.1. All VPs

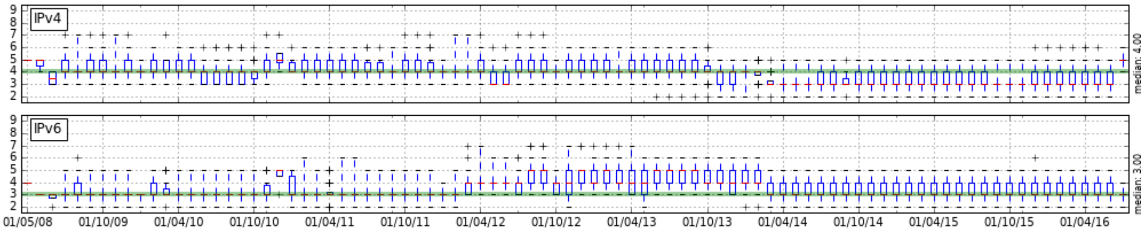


Figure C.1.: Path average length of all peers of A-Root

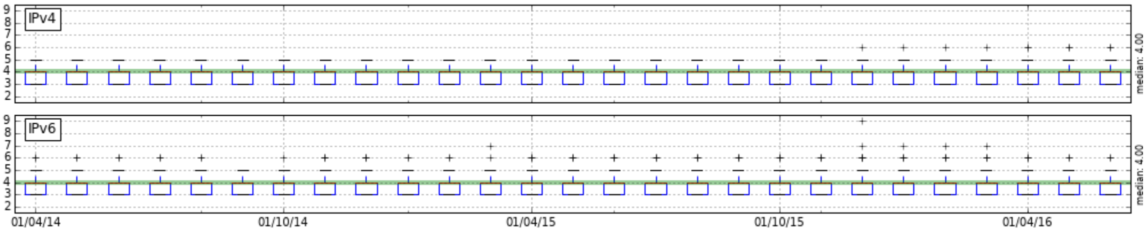


Figure C.2.: Path length distribution of all C-Root's VPs

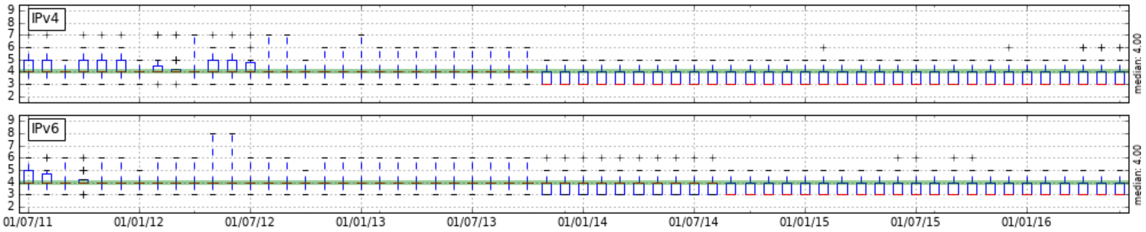


Figure C.3.: Path length distribution of all D-Root's VPs

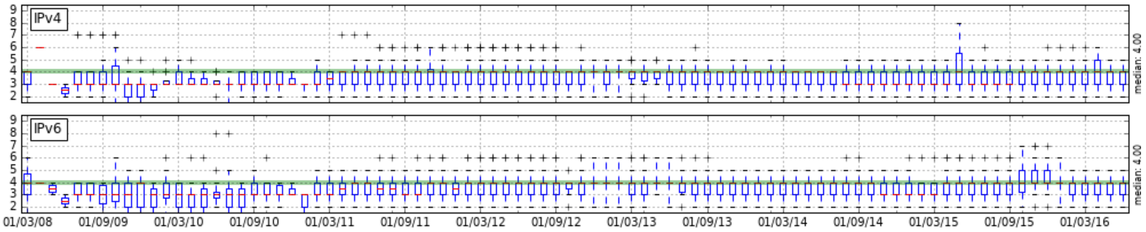


Figure C.4.: Path length distribution of all F-Root's VPs

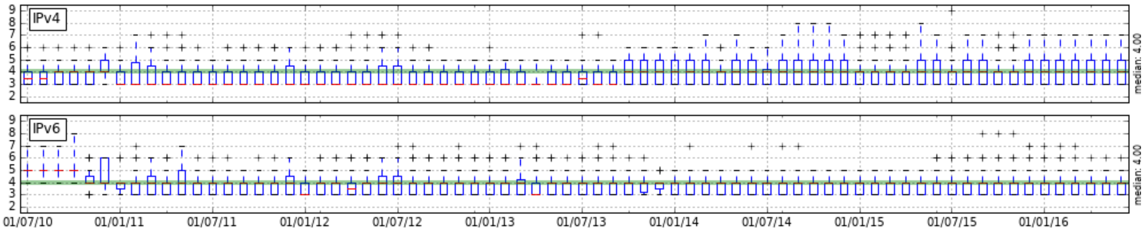


Figure C.5.: Path length distribution of all I-Root's VPs

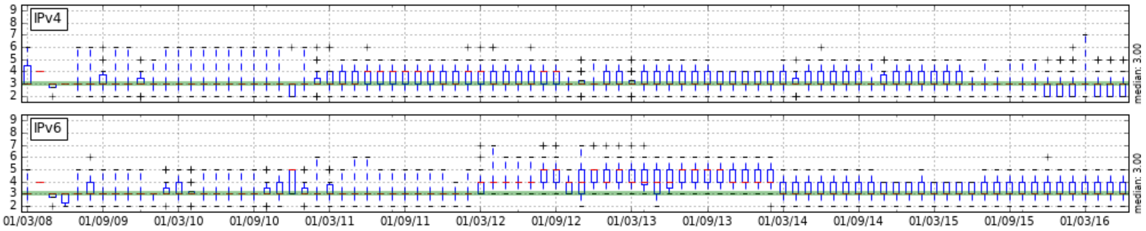


Figure C.6.: Path length distribution of all J-Root's VPs

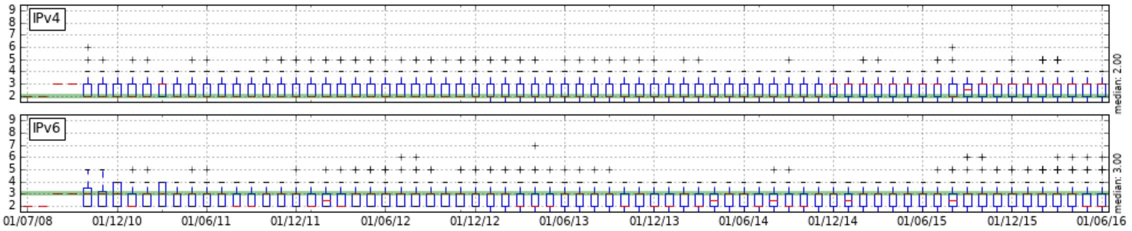


Figure C.7.: Path length distribution of all K-Root's VPs

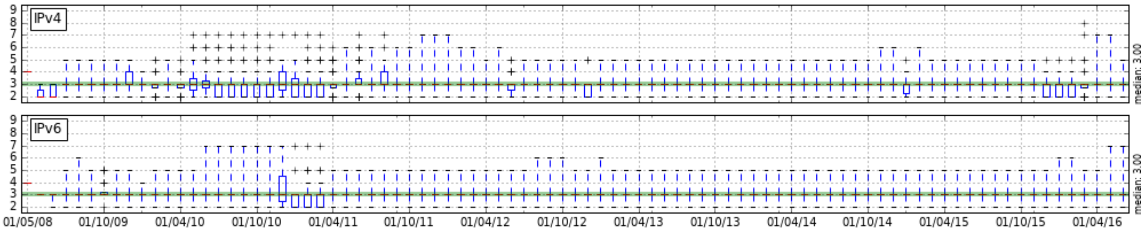


Figure C.8.: Path length distribution of all L-Root's VPs

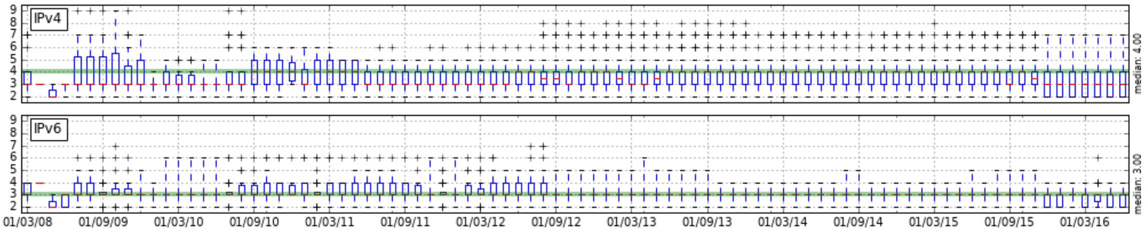


Figure C.9.: Path length distribution of all M-Root's VPs

C.2. Only for VPs with Diverging IPv4/IPv6 Paths

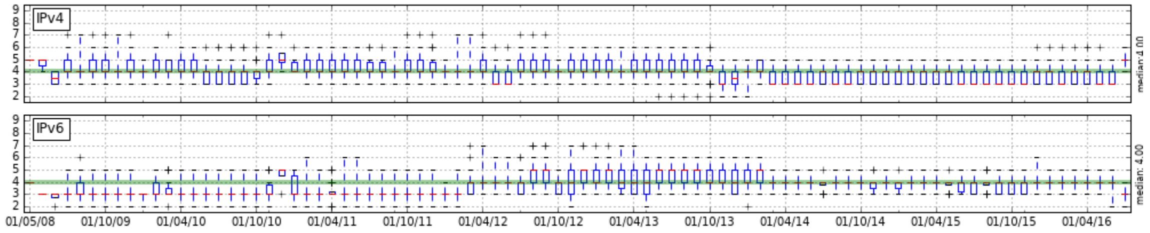


Figure C.10.: Average path length of A-Root peers that have different IPv4/IPv6 paths

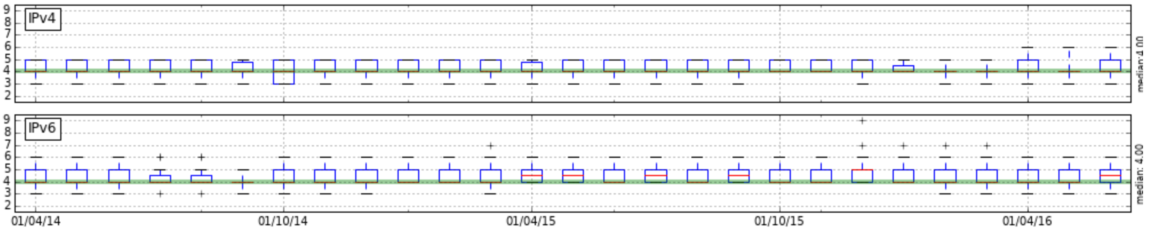


Figure C.11.: Average path length of C-Root peers that have different IPv4/IPv6 paths

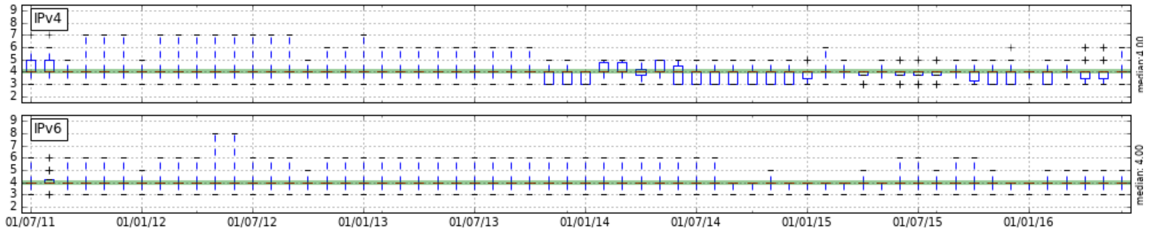


Figure C.12.: Average path length of D-Root peers that have different IPv4/IPv6 paths

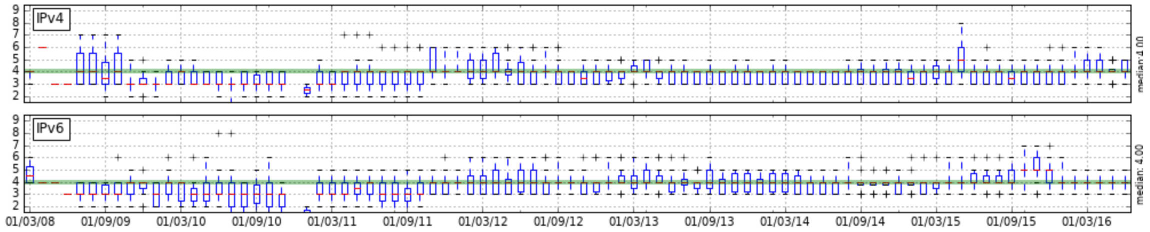


Figure C.13.: Average path length of F-Root peers that have different IPv4/IPv6 paths

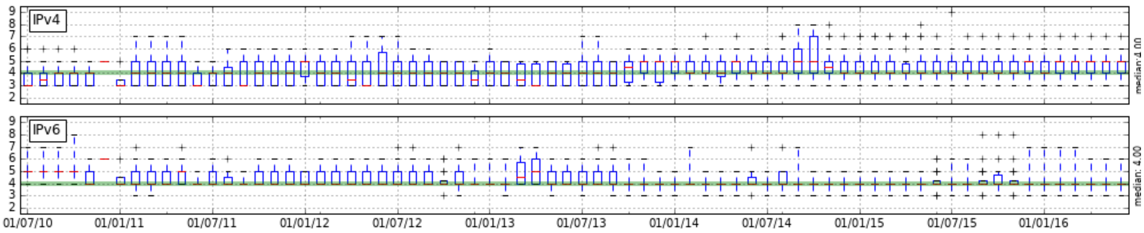


Figure C.14.: Average path length of I-Root peers that have different IPv4/IPv6 paths

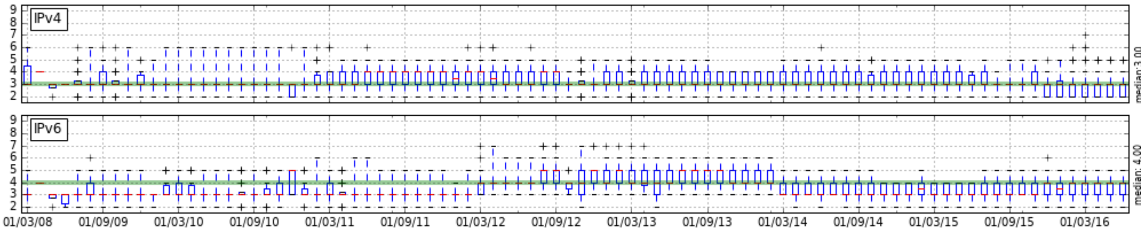


Figure C.15.: Average path length of J-Root peers that have different IPv4/IPv6 paths

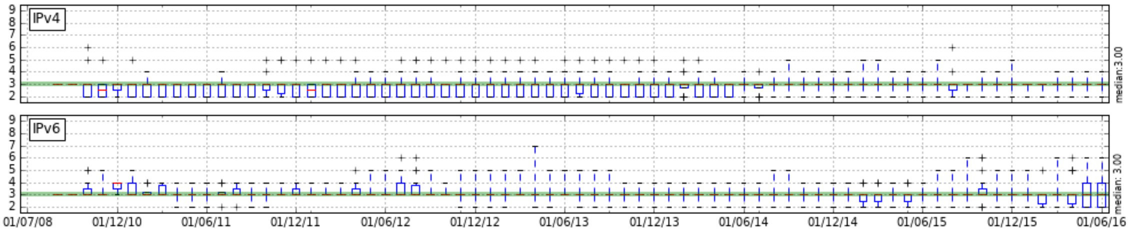


Figure C.16.: Average path length of K-Root peers that have different IPv4/IPv6 paths

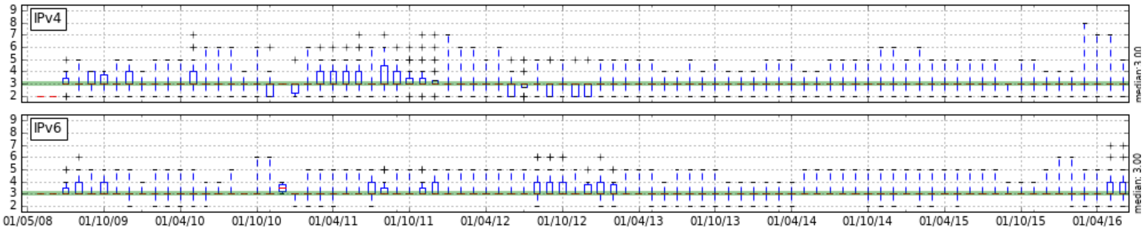


Figure C.17.: Average path length of L-Root peers that have different IPv4/IPv6 paths

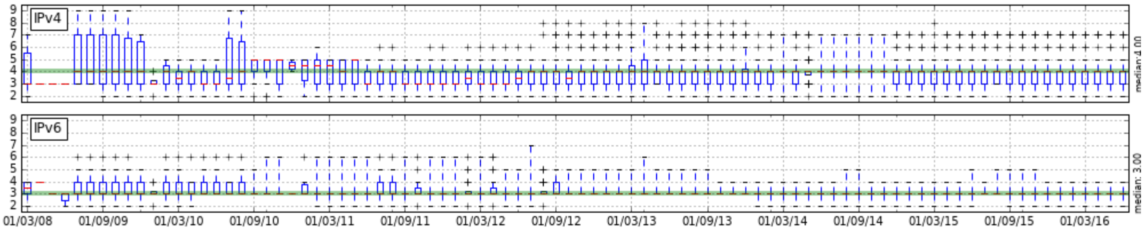


Figure C.18.: Average path length of M-Root peers that have different IPv4/IPv6 paths

D. VP Length Degree

The Root Server's diverging VPs

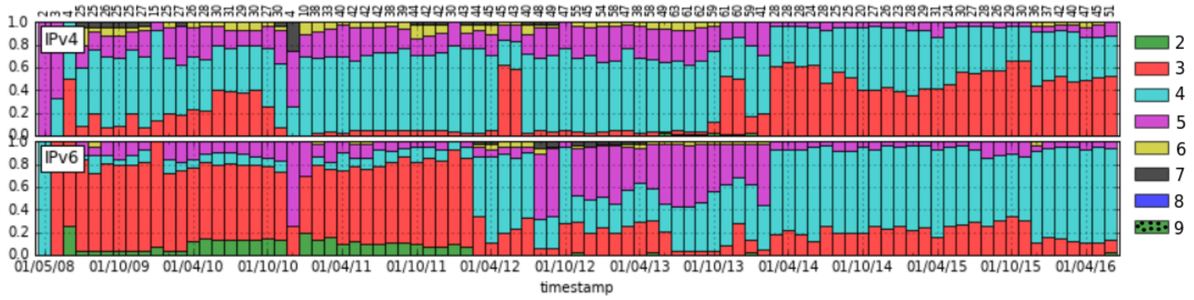


Figure D.1.: VP degree distribution of A-Root

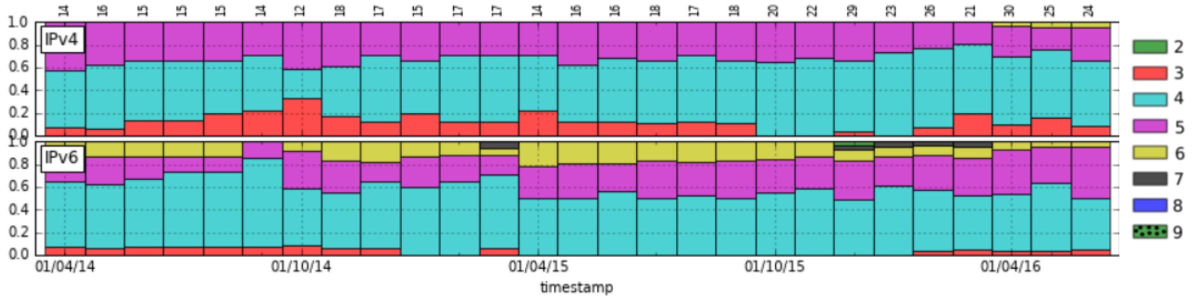


Figure D.2.: VP degree distribution of C-Root

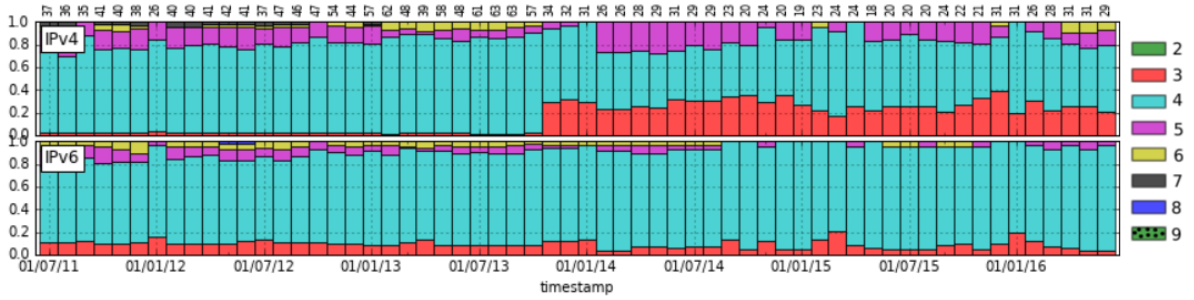


Figure D.3.: VP degree distribution of D-Root

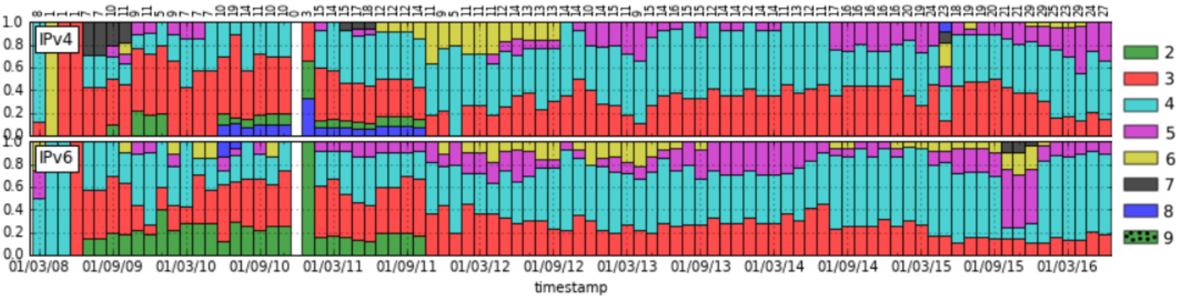


Figure D.4.: VP degree distribution of F-Root

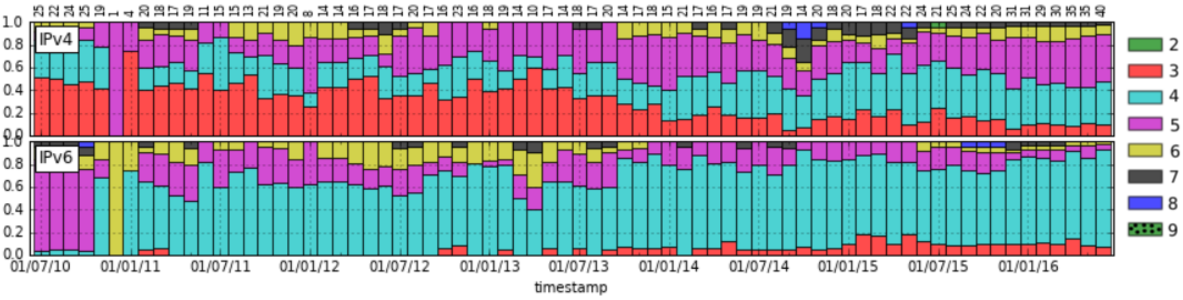


Figure D.5.: VP degree distribution of I-Root

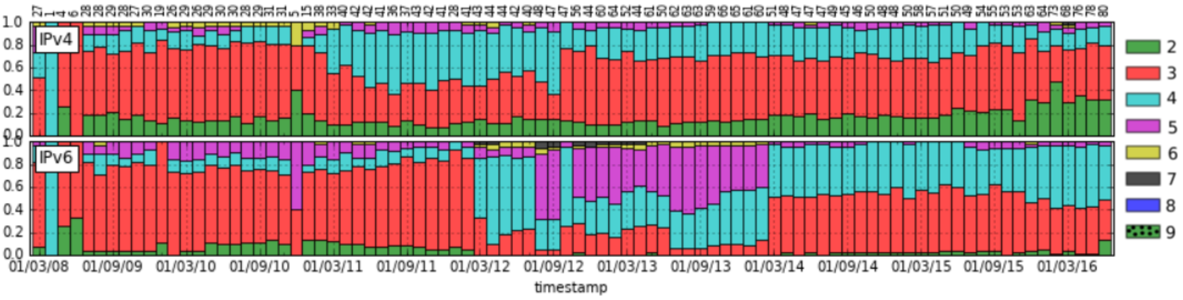


Figure D.6.: VP degree distribution of J-Root

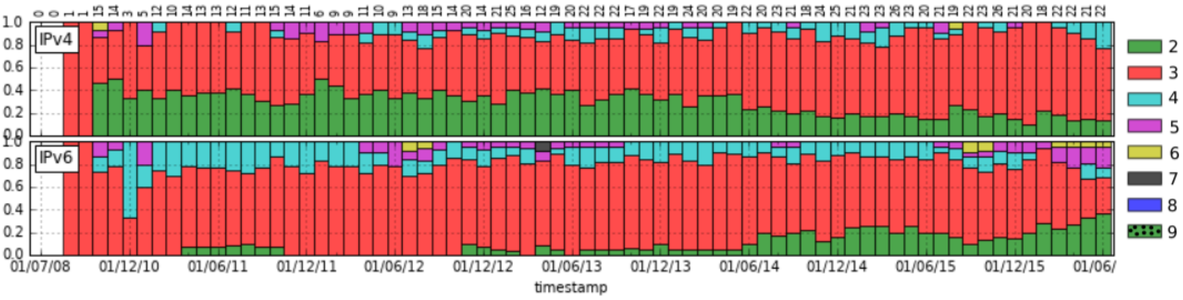


Figure D.7.: VP degree distribution of K-Root

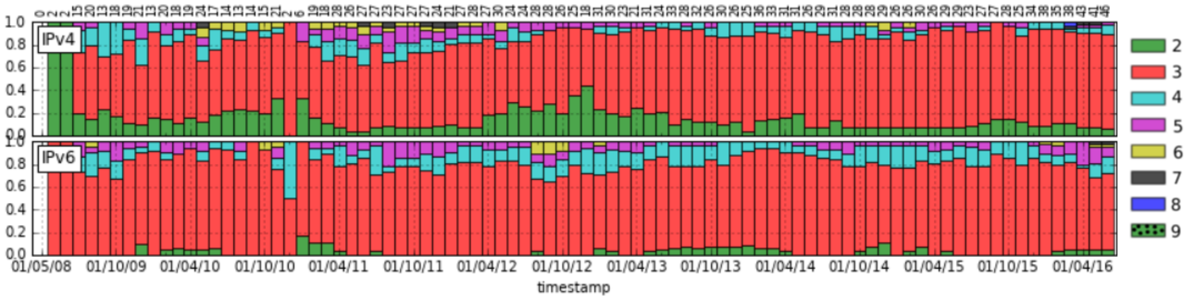


Figure D.8.: VP degree distribution of L-Root

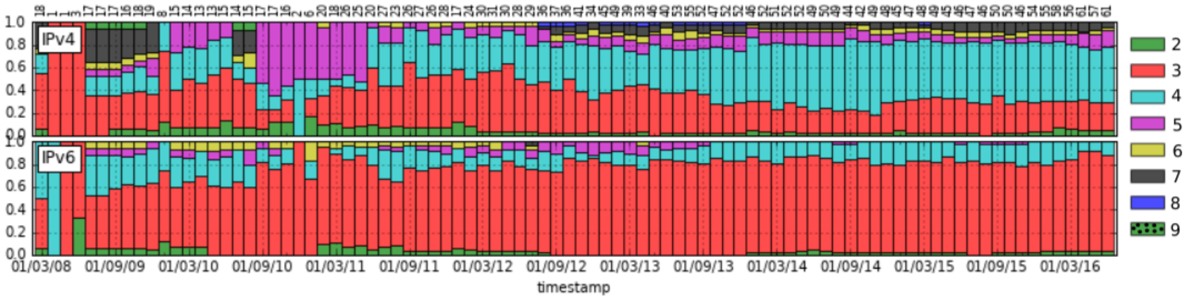


Figure D.9.: VP degree distribution of M-Root

E. Average Path Length Differences for VPs with Shorter IPv4 Path

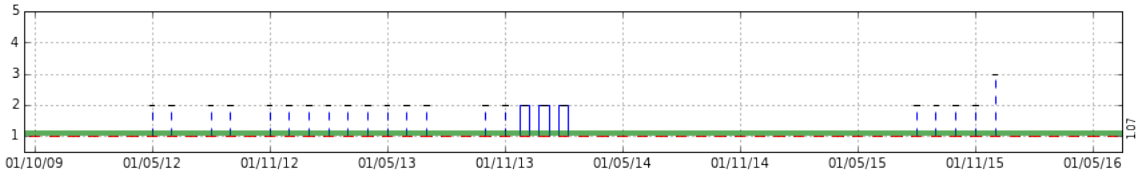


Figure E.1.: Path length differences for A-Root's VPs with shorter IPv4 path

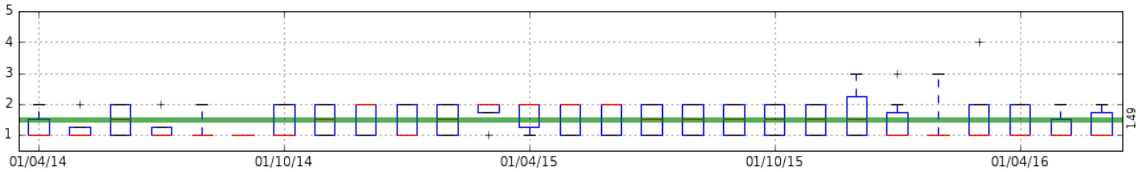


Figure E.2.: Path length differences for C-Root's VPs with shorter IPv4 path

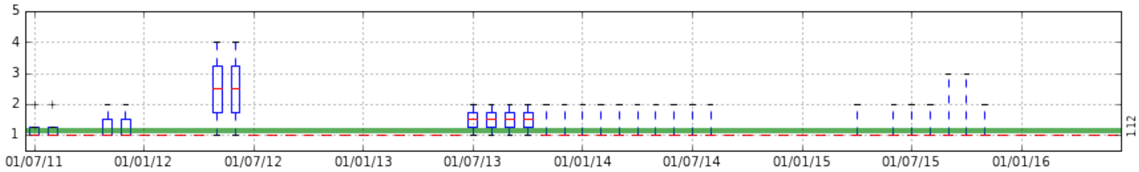


Figure E.3.: Path length differences for D-Root's VPs with shorter IPv4 path

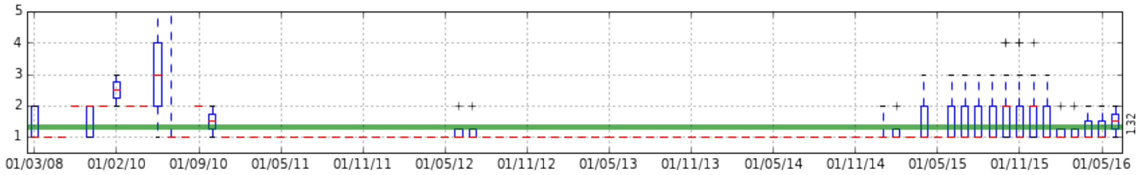


Figure E.4.: Path length differences for F-Root's VPs with shorter IPv4 path

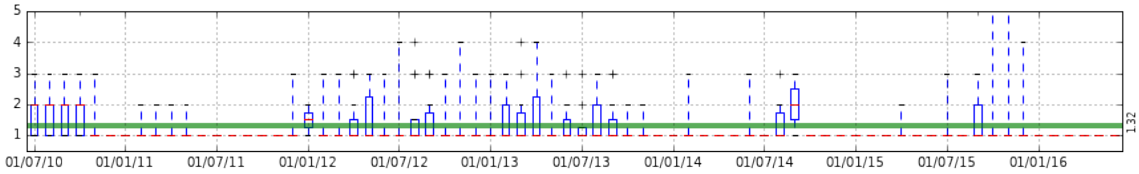


Figure E.5.: Path length differences for I-Root's VPs with shorter IPv4 path

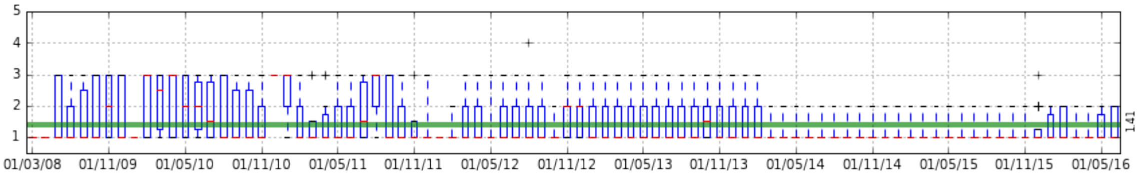


Figure E.6.: Path length differences for J-Root's VPs with shorter IPv4 path

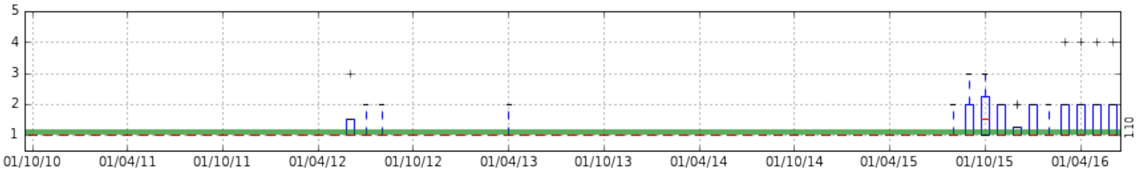


Figure E.7.: Path length differences for K-Root's VPs with shorter IPv4 path

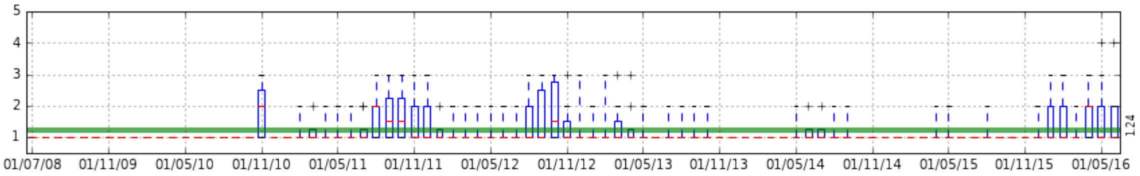


Figure E.8.: Path length differences for L-Root's VPs with shorter IPv4 path

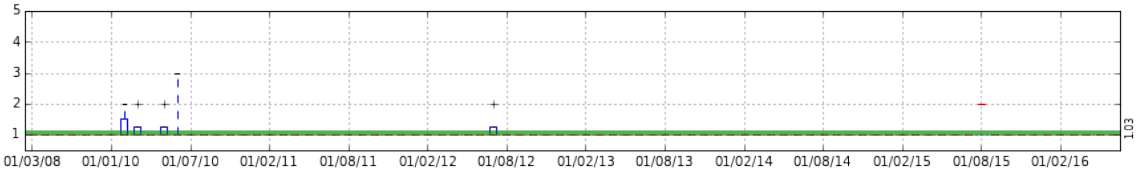


Figure E.9.: Path length differences for M-Root's VPs with shorter IPv4 path

F. Average Path Length Differences for VPs with Shorter IPv6 Path

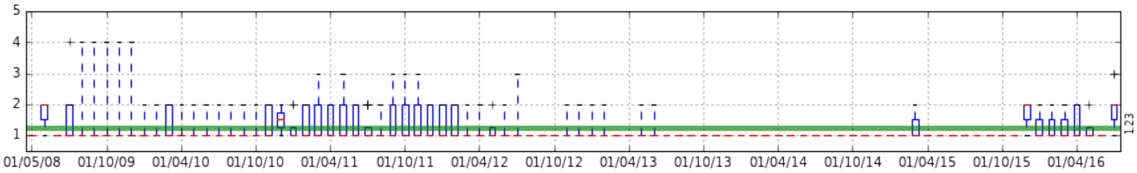


Figure F.1.: Path length differences for A-Root's VPs with shorter IPv6 path

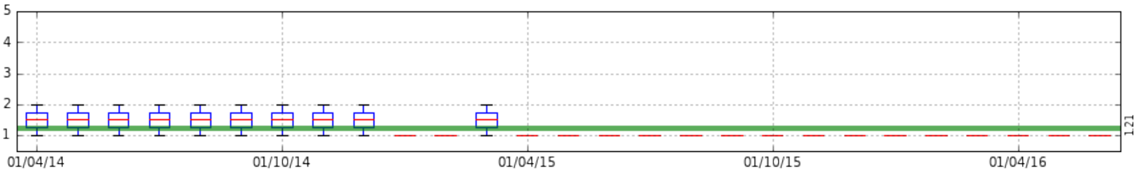


Figure F.2.: Path length differences for C-Root's VPs with shorter IPv6 path

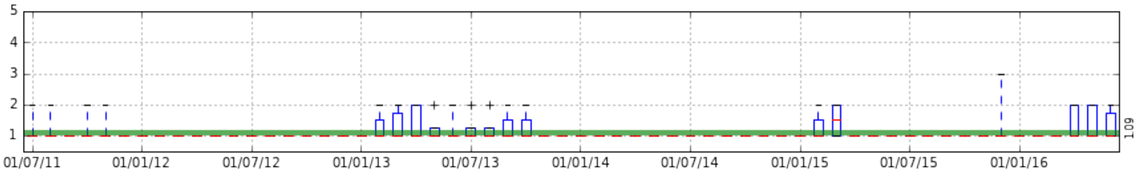


Figure F.3.: Path length differences for D-Root's VPs with shorter IPv6 path

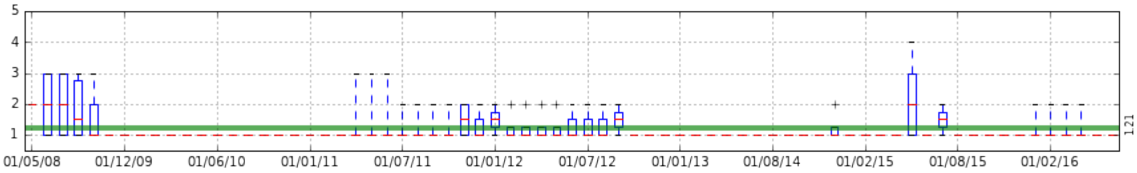


Figure F.4.: Path length differences for F-Root's VPs with shorter IPv6 path

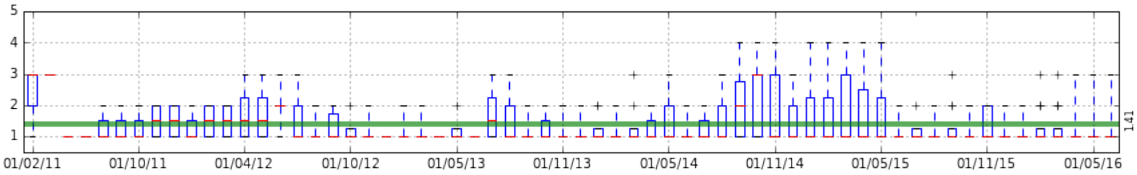


Figure F.5.: Path length differences for I-Root's VPs with shorter IPv6 path

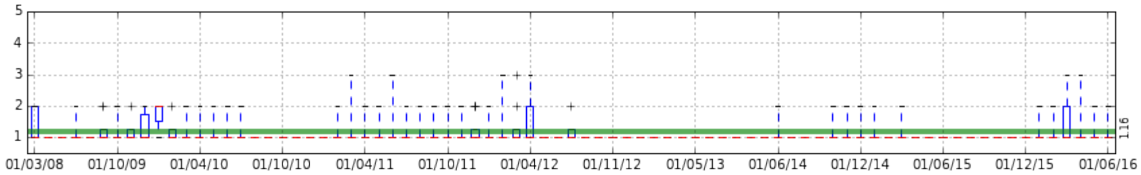


Figure F.6.: Path length differences for J-Root's VPs with shorter IPv6 path

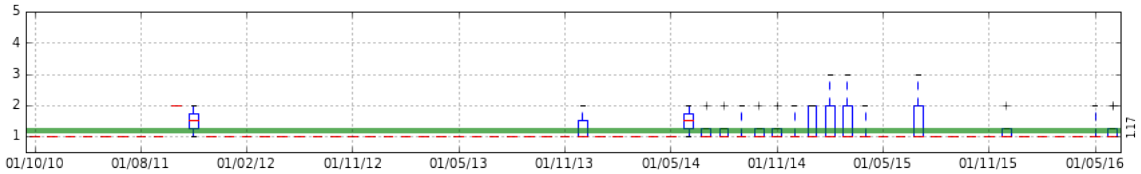


Figure F.7.: Path length differences for K-Root's VPs with shorter IPv6 path

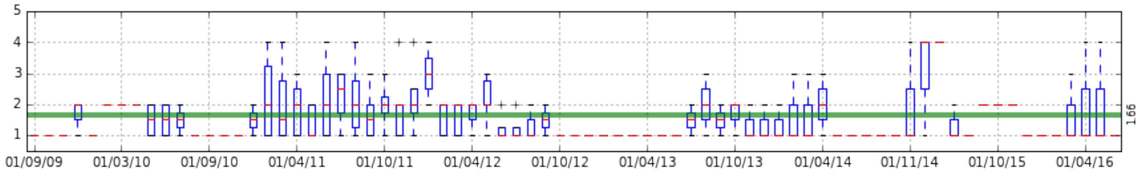


Figure F.8.: Path length differences for L-Root's VPs with shorter IPv6 path

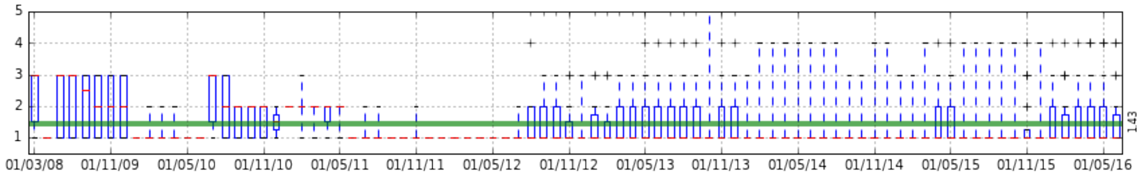


Figure F.9.: Path length differences for M-Root's VPs with shorter IPv6 path

Bibliography

[1] *A Border Gateway Protocol 4 (BGP-4)*. URL: https://www.ietf.org/rfc/rfc4271.txt.

[2] J. Abley and K. Lindqvist. *Operation of Anycast Services*. URL: https://tools.ietf.org/html/rfc4786.

[3] Christopher Amin et al. "Visualization and Monitoring for the Identification and Analysis of DNS Issues". In: *The Tenth International Conference on Internet Monitoring and Protection* (2015).

[4] *Anycast DNS Monitoring Framework*. URL: https://github.com/wicaksana/anycast-dns-monitoring-framework.

[5] *Anycast illustration*. URL: https://upload.wikimedia.org/wikipedia/commons/thumb/4/43/Anycast.svg/320px-Anycast.svg.png.

[6] V. Bajpai and J. Schönwälder. "IPv4 versus IPv6 - who connects faster?" In: *IFIP Networking Conference (IFIP Networking), 2015*. 2015, pp. 1–9. DOI: 10.1109/IFIPNetworking.2015.7145323.

[7] Hitesh Ballani, Paul Francis, and Sylvia Ratnasamy. "A Measurement-based Deployment Proposal for IP Anycast". In: *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*. IMC '06. Rio de Janeriro, Brazil: ACM, 2006, pp. 231–244. ISBN: 1-59593-561-4. DOI: 10.1145/1177080.1177109. URL: http://doi.acm.org/10.1145/1177080.1177109.

[8] Piet Barber et al. "Life and times of J-ROOT". In: *Proceedings of NANOG*. Vol. 32. 2004.

[9] *BGPlay*. URL: http://www.dia.uniroma3.it/~compunet/www/view/tool.php?id=bgplay.

[10] *BGPlay.js*. URL: http://bgplayjs.com/.

[11] *BGPMon*. URL: http://www.bgpmon.io/.

[12] S. Bhattacharjee et al. "Application-layer anycasting". In: *INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE*. Vol. 3. 1997, 1388–1396 vol.3. DOI: 10.1109/INFCOM.1997.631176.

[13] Peter Boothe and Randy Bush. "DNS Anycast Stability". In: *19th APNIC,'05* (2005).

[14] *Caida OpenBMP*. URL: https://bgpstream.caida.org/data#!caida-bmp.

[15] Matt Calder et al. "Analyzing the Performance of an Anycast CDN". In: *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*. IMC '15. Tokyo, Japan: ACM, 2015, pp. 531–537. ISBN: 978-1-4503-3848-6. DOI: 10.1145/2815675.2815717. URL: http://doi.acm.org/10.1145/2815675.2815717.

[16] Yi-Ching Chiu et al. "Are We One Hop Away from a Better Internet?" In: *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*. IMC '15. Tokyo, Japan: ACM, 2015, pp. 523–529. ISBN: 978-1-4503-3848-6. DOI: 10.1145/2815675.2815719. URL: http://doi.acm.org/10.1145/2815675.2815719.

[17] Danilo Cicalese et al. "A First Look at Anycast CDN Traffic". In: *arXiv preprint arXiv:1505.00946* (2015).

[18] Danilo Cicalese et al. "A fistful of pings: Accurate and lightweight anycast enumeration and geolocation". In: *Computer Communications (INFOCOM), 2015 IEEE Conference on*. IEEE. 2015, pp. 2776–2784.

[19] Danilo Cicalese et al. "Characterizing IPv4 Anycast Adoption and Deployment". In: (2015).

[20] Danilo Cicalese et al. *Latency-Based Anycast Geolocalization: Algorithms, Software and Datasets*. Tech. rep. Tech. Rep, 2015.

[21] Lorenzo Colitti et al. "Evaluating the effects of anycast on DNS root name servers". In: *RIPE document RIPE-393* 6 (2006).

[22] Autonomic Computing. "An architectural blueprint for autonomic computing". In: *IBM Publication* (2003).

[23] Jakub Czyz et al. "Measuring IPv6 Adoption". In: *Proceedings of the 2014 ACM Conference on SIGCOMM*. SIGCOMM '14. Chicago, Illinois, USA: ACM, 2014, pp. 87–98. ISBN: 978-1-4503-2836-4. DOI: 10.1145/2619239.2626295. URL: http://doi.acm.org/10.1145/2619239.2626295.

[24] F. Scalszo D. McPherson R. Donnelly. *Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services*. URL: https://tools.ietf.org/html/rfc6382.

[25] *D3.js*. URL: https://d3js.org/.

[26] L. Deri et al. "A distributed DNS traffic monitoring system". In: *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*. 2012, pp. 30–35. DOI: 10.1109/IWCMC.2012.6314173.

[27] Amogh Dhamdhere et al. "Measuring the Deployment of IPv6: Topology, Routing and Performance". In: *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*. IMC '12. Boston, Massachusetts, USA: ACM, 2012, pp. 537–550. ISBN: 978-1-4503-1705-4. DOI: 10.1145/2398776.2398832. URL: http://doi.acm.org/10.1145/2398776.2398832.

[28] *Factsheet: Root server attack on 6 February 2007*. URL: https://www.icann.org/en/system/files/files/factsheet-dns-attack-08mar07-en.pdf.

[29] Xun Fan, J. Heidemann, and R. Govindan. "Evaluating anycast in the domain name system". In: *INFOCOM, 2013 Proceedings IEEE*. 2013, pp. 1681–1689. DOI: 10.1109/INFCOM.2013.6566965.

[30] Xun Fan, John Heidemann, and Ramesh Govindan. *Identifying and characterizing anycast in the domain name system*. Tech. rep. Tech. rep, 2011.

[31] Steve Gibbard and Packet Clearing House. *Observations on anycast topology and performance*. Tech. rep. Packet Clearing House, 2007.

[32] Enrico Gregori et al. "On the Incompleteness of the AS-level Graph: A Novel Methodology for BGP Route Collector Placement". In: *Proceedings of the 2012 ACM Conference on Internet Measurement Conference*. IMC '12. Boston, Massachusetts, USA: ACM, 2012, pp. 253–264. ISBN: 978-1-4503-1705-4. DOI: 10.1145/2398776.2398803. URL: http://doi.acm.org/10.1145/2398776.2398803.

[33] James Hiebert et al. "Determining the cause and frequency of routing instability with anycast". In: *Technologies for Advanced Heterogeneous Networks II*. Springer, 2006, pp. 172–185.

[34] *How BGP Works*. URL: http://www.slideshare.net/ThousandEyes/how-bgp-works.

[35] *IPv4 and IPv6 AS Core: Visualizing IPv4 and IPv6 Internet Topology at a Macroscopic Scale*. URL: http://www.caida.org/research/topology/as_core_network/.

[36] S.Stuart J. Scudder R. Fernando. *BGP Monitoring Protocol draft-ietf-grow-bmp-17*. URL: https://tools.ietf.org/html/draft-ietf-grow-bmp-17.

[37] Daniel Karrenberg. "Anycast and BGP Stability:A Closer Look at DNSMON Data". In: *Proceedings of NANOG37* 11 (2005).

[38] J.H. Kuipers. *Analysing the K-root Anycast Infrastructure*. URL: https://labs.ripe.net/Members/jh_kuipers/analyzing-the-k-root-anycast-infrastructure.

[39] M. Kühne. *Update on AS Path Lengths Over Time*. URL: https://labs.ripe.net/Members/mirjam/update-on-as-path-lengths-over-time.

[40] C. Labovitz L. Blunk M. Karir. *Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format*. URL: https://tools.ietf.org/html/rfc6396.

[41] Bu-Sung Lee et al. "Availability and effectiveness of root DNS servers: A long term study". In: *Network Operations and Management Symposium (NOMS), 2010 IEEE*. 2010, pp. 862–865. DOI: 10.1109/NOMS.2010.5488355.

[42] Matt Levine, Barrett Lyon, and Todd Underwood. "Operational experience with TCP and Anycast". In: *Presentation and Q&A given at NANOG* 37 (2006).

[43] Ziqian Liu et al. "Two days in the life of the DNS anycast root servers". In: *Passive and Active Network Measurement*. Springer, 2007, pp. 125–134.

[44] Doug Madory, Chris Cook, and Kevin Miao. "Who Are the Anycasters?" In: *Proceedings of NANOG59* 10 (2013).

[45] P. Mockapetris. *Domain Names - Concepts and Facilities*. URL: https://tools.ietf.org/html/rfc1034.

[46] P. Mockapetris. *Domain Names - Implementation and Specification*. URL: https://tools.ietf.org/html/rfc1035.

[47] M. Nikkhah and R. Guérin. "Migrating the Internet to IPv6: An Exploration of the When and Why". In: *IEEE/ACM Transactions on Networking* PP.99 (2016), pp. 1–1. ISSN: 1063-6692. DOI: 10.1109/TNET.2015.2453338.

[48] *Open BGP Monitoring Protocol (OpenBMP) Collection Framework*. URL: http://www.openbmp.org/.

[49] *Packet Clearing House BGP Routing Resources*. URL: https://www.pch.net/resources/.

[50] C. Partridge, T. Mendez, and W. Miliken. *Host Anycasting Service*. URL: https://tools.ietf.org/html/rfc1546.

[51] *PEERING - The BGP Testbed*. URL: https://peering.usc.edu/about/.

[52] E. M. Reingold and J. S. Tilford. "Tidier Drawings of Trees". In: *IEEE Transactions on Software Engineering* SE-7.2 (1981), pp. 223–228. ISSN: 0098-5589. DOI: 10.1109/TSE.1981.234519.

[53] *RIPE Routing Information Service (RIS)*. URL: https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris.

[54] *RIPEstat*. URL: https://stat.ripe.net/.

[55] *Root nameservers official website*. URL: http://www.root-servers.org/.

[56] M. Roughan et al. "10 Lessons from 10 Years of Measuring and Modeling the Internet's Autonomous Systems". In: *IEEE Journal on Selected Areas in Communications* 29.9 (2011), pp. 1810–1821. ISSN: 0733-8716. DOI: 10.1109/JSAC.2011.111006.

[57] Sandeep Sarat, Vasileios Pappas, and Andreas Terzis. "On the use of anycast in DNS". In: *Computer Communications and Networks, 2006. ICCCN 2006. Proceedings. 15th International Conference on*. IEEE. 2006, pp. 71–78.

[58] R. Schmidt et al. *IP Anycasting: Understanding routing impact of adding/removing instances*. URL: https://github.com/CAIDA/bgp-hackathon/tree/anycast.

[59] *University of Oregon Route Views Project*. URL: http://www.routeviews.org/.

[60] P. Vixie, G. Sneeringer, and M. Schleifer. *Events of 21-Oct-2002*. URL: http://c.root-servers.org/october21.txt.

[61] *VizAS*. URL: https://labs.apnic.net/vizas/.

[62] S. Wolf and D. Conrad. *Requirements for a Mechanism Identifying a Name Server Instance*. URL: https://www.ietf.org/rfc/rfc4892.txt.

[63] Yingdi Yu et al. "Measuring the Placement of DNS Servers in Top-Level-Domain". In: ().